ON GLITCHKRIEGE:

Strategy in the Cyber-Age

BY

LIEUTENANT-COLONEL WILLIAM DUPUY

FRENCH AIR FORCE

A THESIS PRESENTED TO THE FACULTY OF
THE SCHOOL OF ADVANCED AIR AND SPACE STUDIES
FOR COMPLETION OF GRADUATION REQUIREMENTS

SCHOOL OF ADVANCED AIR AND SPACE STUDIES
AIR UNIVERSITY
MAXWELL AIR FORCE BASE, ALABAMA
JUNE 2013

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
JUN 2013		**00-00-2013 to 00-00-2013**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
On Glitchkriege: Strategy in the Cyber-Age	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **School Of Advanced Air And Space Studies,,Air University,,Maxwell Air Force Base,,AL**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

The steady growth of the strategic significance of cyberspace has disconcerted politicians, international relations specialists and military strategists alike. Indeed, its characteristics make a direct application of the respective knowledge of these groups at least uneasy, at most impossible. To make the matter worse, no single theory of cyberpower has reached academic consensus. The purpose of this thesis, therefore, is to draft a theory of cyberspace strategy: it is wholly focused on the exertion of violence through cyberspace in pursuance of political outcomes. This end motivated the structure of this document. This intellectual journey explicitly aimed at examining the extent to which existing knowledge of international politics and of general military strategy could inform strategy in cyberspace. It concluded that they can apply if the characteristics these fields of study manipulate are correctly interpreted in cyberspace. Coming to that conclusion required an extensive analysis.

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**124**	

APPROVAL

The undersigned certify that this thesis meets master's-level standards of research, argumentation, and expression.

_____

SUZANNE C. BUONO (Date)

_____

EVERETT C. DOLMAN (Date)

DISCLAIMER

The conclusions and opinions expressed in this document are those of the author. They do not reflect the official position of the US or French Governments, Department of Defense, the United States or French Air Force, or Air University.

ABOUT THE AUTHOR

Lieutenant-Colonel William Dupuy entered the French Air Force Academy in 1995 as an engineering officer and graduated in 1998 as a Telecommunications engineer. His first assignment introduced him to the fascinating world of deployable Command and Control centers. After a few years spent installing operational networks in tents and shelters, he gradually moved to more expert duties. He was involved in network architecture for a while before being granted the privilege of studying information security for two years. Finding in cryptography an unexpected opportunity to practice his passion for mathematics, he published a research article that was presented to the annual conference CHES'05.

With his newly acquired academic credentials, he was assigned to the French Center of Military Aerial Experiment (CEAM 00.330) where he was involved in most air force and joint procurement programs—first directly, then as the commandant of the IT security assessment team (EVASSI 17.330). Then he came back to his initial (tactical) duties within the Telecommunication Group GT 10.801 as Operations Officer. He then successfully passed the *Ecole de Guerre* competitive exam and was selected to attend the US Air Force Air Command and Staff College and the School of Advanced Air and Space Studies.

Lieutenant-Colonel William Dupuy owns an engineering degree from the French Air Force Academy, a master's degree from the Information Security Training Center and a master's degree from the Air Command and Staff College.

.

ACKNOWLEDGEMENTS

Writing over a hundred pages of a thesis in a foreign language is a journey you usually do not want to accomplish alone. Fortunately, many supported this undertaking in a variety of ways.

I am grateful to the instructors that have hardened my skin and improved my skills throughout the two years I have spent at the Air University. Indeed, it would be unfair to forget the instructors that had to deal with the terrible writer I was when I began the ACSC curriculum. I would like to distinguish Dr. John Terino and Dr. William Dean III for their mentoring.

Getting used to the American way of PME was hard in ACSC, getting in pace with SAASS battle rhythm was even harder. I am grateful to the whole body of SAASS instructors. Each of them has contributed to some extent to this thesis that reflects a portion of the knowledge I was provided with here.

Among them, two were especially involved. Doctor Everett Dolman, my reader, found the best compromise between the final quality of this document, and the final quality of my comps review. His outstanding editing work truly raised the quality of this thesis to a result that I had not hoped for. As for Colonel Suzanne Buono, she was offered the worst possible gift before she retired: she would have to handle a stubborn French student, having footnotes allergy (and repulsed by everything related to formatting a document) and writing roughly English. Yet, her infectious enthusiasm immunized me from despair and spurred me towards promising directions.

My sponsors were also an outstanding support. Lew's wise assessment of my papers pushed me towards excellence and gave me an idea when to stop working. Tess was a great support to my family for everything ranging from my children's homework to my wife's medical appointments.

Finally, I thank my whole family for their understanding of the ordeal I was going through. They have been an outstanding throughout the year, bearing my changing mood and mental absences.

When I passed the Air Force competitive exam, a colonel congratulated my wife, not me, for the success. Today I understand the extent to which she is an actor of all my achievements, and this one in particular.

ABSTRACT

The steady growth of the strategic significance of cyberspace has disconcerted politicians, international relations specialists and military strategists alike. Indeed, its characteristics make a direct application of the respective knowledge of these groups at least uneasy, at most impossible. To make the matter worse, no single theory of cyberpower has reached academic consensus. The purpose of this thesis, therefore, is to draft a theory of cyberspace strategy: it is wholly focused on the exertion of violence through cyberspace in pursuance of political outcomes. This end motivated the structure of this document. This intellectual journey explicitly aimed at examining the extent to which existing knowledge of international politics and of general military strategy could inform strategy in cyberspace. It concluded that they can apply if the characteristics these fields of study manipulate are correctly interpreted in cyberspace. Coming to that conclusion required an extensive analysis.

Defining and circumscribing cyberspace conditions its integration into existing strategies. Accordingly, I defined cyberspace in a way that does not interfere with existing domains and subsequent strategies, which required clarification on the notion of domain and its use in strategy and international politics.

The purpose of cyberspace strategy stems from its utility in international politics. Given that violence expresses itself very differently in cyberspace, an overview of the mechanisms linking the exertion of violence with political effects is a necessary preamble to analyzing strategy. To illustrate the mechanisms of bargaining, I studied specifically the mechanisms of coercion.

Military strategy eventually seeks to produce political effects, but it usually requires overcoming enemy resistance first. The characterization of strategy in Chapter 3 describes this process, analyzes the intertwining of two strategies and explains how leaders mitigate enemy uncertainty.

This analysis eventually underpins the analysis of cyberspace strategy offered in Chapter 4. The characteristics of violence in cyberspace define the range of effects cyber-conflicts can produce, while the characteristics of cyberspace tactics shape cyberspace strategy. Finally, grand cyber-strategy addresses the shaping of a cyber-environment that maximizes national advantage.

Contents

DISCLAIMER **2**
ABOUT THE AUTHOR **3**
ACKNOWLEDGEMENTS **4**
ABSTRACT **5**
Introduction **6**
Chapter 1 Cyber Strategy: Evolution Or Revolution? **12**
Chapter 2 Force in International Politics **36**
Chapter 3 Timeless Strategy **54**
Chapter 4 A Strategy of Bits and Peaces **83**
Conclusion **110**
BIBLIOGRAPHY **117**

Introduction

The history of communication and computation merged on 29 October 1969, with the first digital communication attempt on the campus of UCLA's School of Engineering and Applied Science, Menlo Park, California.[1] Since then, the level of connectivity between computing devices has steadily increased. In addition, computerized devices have flooded human life and permeated social practices.

Yet, this development has hardly followed a conscious pattern. Growing following a liberal ideal, it has mostly developed anarchically, led by consumers' needs and fancy and private companies' impulses. Initially minimally involved, states are gradually forced to acknowledge its growing political, economic, and social significance. Indeed, industry commercial transactions and financial exchanges are increasingly dependent on digital networks for their effectiveness and reliability. In addition, social media have proved a significant political influence, creating new relationships between the peoples and their rulers.[2]

---

[1] (Barry M. Leiner et al., "A Brief History of the Internet" (1999), http://arxiv.org/abs/cs/9901011 (accessed April 14, 2013).

[2] In Evgeny Morozov, *The Net Delusion: The Dark Side of Internet Freedom* (New York: PublicAffairs, 2012), 113-115. Evgeny Morozov showed that many authoritarian states sought to pervert the liberal ideal that motivated the growth of the Internet to protect their regime. Even in that case though, the exchanges between a dictator and his people evolved. Thus Morozov describes how Venezuelan dictator Hugo Chavez exploited social media to further their propaganda. Thus, although the mechanics of politics apply in this medium, it proves an increasingly critical environment.

Disruption of national activities from cyberspace takes several forms. Cyber-criminality induces a direct cost to companies and individuals, but the indirect costs (for instance defense expenses) are even more significant.[3] Terrorist organizations take advantage of the opportunities in cyberspace to recruit, train, and organize.[4] Some states, finally, spy on their counterparts and absorb informational wealth, and consider harming their competitors through massive cyber-attacks.[5]

Cyberspace also provides states with new strategic opportunities of exertion of violence. Cyber-attacks are stealthy and plausibly deniable; they usually do not provoke massive civilian casualties and do not violate territorial sovereignty.[6] In addition, the international community acknowledges their nuisance but deems them relatively more benign than their kinetic equivalent. For all these reasons, states are enticed to invest this new environment.

Unfortunately, the dynamics of power and violence in cyberspace are still largely misunderstood. None of the traditional mechanisms of power building and exertion apply adequately in cyberspace. A variety of

---

[3] For an example of characterization of the global cost of cybercrime, see Ross Anderson et al., "Measuring the Cost of Cybercrime," in *11th Workshop on the Economics of Information Security* (June), 2012, http://lyle.smu.edu/~tylerm/Iis12pres.pdf (accessed April 16, 2013).
[4] Thomas Rid and Marc Hecker, *War 2.0: Irregular Warfare in the Information Age* (Westport, CO: Praeger Security International, 2009). Kindle reader e-book
[5] Joel Brenner, *America the Vulnerable: Inside the New Threat Matrix of Digital Espionage, Crime, and Warfare* (New York: Penguin, 2011), 70; Richard A Clarke and Robert K Knake, *Cyber-War: What It Is and How to Fight It* (New York: Ecco, 2010), 31.
[6] Martin C. Libicki, "Sub Rosa Cyber-War," *The Virtual Battlefield: Perspectives on Cyber-Warfare* 3 (2009): 6.

states and non-state actors interact in every aspect of cyber-activities. Consequently, the spectrum of side effects of any action in cyberspace must be considered globally. Moreover, the expression of power in cyberspace is so intangible that no attempt at theorizing about it has met consensus.[7]

Warfare has not been left unchanged by the advent of cyberspace either. The American Revolution in Military Affairs (RMA) tried to take the best advantage of the progresses of Information and Communication Technologies (ICT) to make the military a more lethal weapon.[8] Nevertheless, it addresses but a secondary aspect of cyber-strategy. Many societal and state interests lie in cyberspace and the effect of their destruction or disruption on conflict resolution and military strategy are still to be understood. In addition, the conflicts escape the battlefield to go into the international stage, the public opinion, and the combatants' homelands. The many interactions taking place in cyberspace during conflicts require a model to explain and offer a base for strategies to develop.

It is the purpose of this document to draft a theory of cyber-strategy. The approach I adopted aimed in essence at bringing the work

---

[7] Franklin D. Kramer, Stuart H Starr, and Larry K Wentz, eds., *Cyberpower and National Security: Policy Recommendations for a Strategic Framework* (Washington, DC: Potomac Books, 2009), xv.
[8] David J. Lonsdale, *The Nature of War in the Information Age: Clausewitzian Future* (New York: Frank Cass, 2004), 7–9.

of several theorists to the level of abstraction required for a transposition of their thought into cyberspace.

Prior to any discussion on cyber-strategy, it is essential to characterize and circumscribe the field of study. Part 1 offers a panorama of existing definitions of cyberspace and selects one that allows a comparison of cyber-strategy to strategy in other domains. This part eventually advocates that existing international politics theory and military theory do not blindly apply to cyberspace, thereby justifying the relevance of this study.

The canons of international politics highlight the mechanisms that transform military might into political advantage. Part 2 focuses on the mechanisms that transform violence into political change. It investigates the mechanisms of coercion to illustrate how bargaining and violence intertwine to decide of the outcomes of conflicts.

These mechanisms define the purpose of strategy. It was then possible in part 3 to delve into the machinery of strategy. Observing that some characteristics of strategy deeply influenced its conduct, I constructed a model that drew inspiration from several military theorists and accounted for these characteristics. Finally, I explained how the variables highlighted in part 3 translated in cyberspace. This process emphasized several lessons for the cyber-strategist. In particular, it demonstrated the range of effects of cyber-attacks. It showed how some

principles of military strategy could apply in cyber-conflicts. Finally, it issued some principles for the building of cyberpower.

Chapter 1

Cyber Strategy: Evolution or Revolution?

The emergence of massively interconnected computers has slowly but radically transformed societies. People communicate, buy, and meet on the Internet; companies do business and finance; knowledge is more available to researchers, citizens, and individuals than it has ever been. And there is more. Our houses get increasingly connected and smart. There are computation devices everywhere: our washing machines, phones (I can question whether they still deserve this name), televisions. Cyberspace has subsequently shaped societal habits: the way people meet and communicate, think, acquire knowledge. It has also modified international politics and international laws, forcing one to wonder what territorial authority means in a borderless environment. Finally, it also poses new defense opportunities and threats: it has provided warfighters with an unprecedented level of tactical information, communication, and therefore flexibility, but it has also empowered new actors and blurred the norms of conflict.

Defining cyberspace is a critical preamble to thinking about cyberspace strategy in several respects. It must account for cyberspace specificities, delimit its borders and define the interactions with other areas of human activities. It also informs the strategist on the relevance

of a specific domain strategy and precedes states' military organization. Accordingly, my purpose is to define cyberspace in a way that demarcates a functionally homogeneous environment. In addition, this definition must circumscribe an environment that does not encroach upon existing warfighting domains or states' instruments of power.

After a short explanation of the soundness of thinking about cyberspace as a separate medium, this part describes the characteristics that are expected from a medium, and from a domain. Accordingly, a definition of cyberspace that would allow defining cyberspace as a domain is offered. Finally, it shows that some unprecedented characteristics of cyberspace require a review of the strategic paradigm.

Emergence of Cyberspace

A rather unique fact, the word "cyberspace" appeared even before its materialization.[1] Indeed, cyberspace came to existence because of the convergence of digital computing and communications, legitimizing the conceptualization of this loose net as a whole.

The emergence of cyberspace coincides with the advent of the World Wide Web (WWW) in the 1990s.[2] Both computing devices and communication systems existed before, but the advent of the Internet

---

[1] In 1982, William Gibson referred to the cyberspace as a world of mass hallucinations of computer networks. Yet it did not materialize until the early 90s. Derek S. Reveron, ed., *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World* (Washington, DC: Georgetown University Press, 2012), 5.
[2] Reveron, *Cyberspace and National Security*, 5.

Protocol (IP) and the massive circulation of knowledge that the WWW facilitated legitimized the conceptualization of digital networks as a single informational ecosystem.

The first electronic computing devices were really operational during World War 2 (WWII). A team of world-class scientists, among them Alan Turing, developed the Bombas to break the sophisticated code of the German encryption device, Enigma.[3] Electronic communication technologies had existed even before then. Wireless telegraphy, which is digital electronic communication, became an important tactical asset during World War 1 (WWI).[4] Nevertheless, each technology, taken separately, only facilitated specific functions usually performed by human beings.

The advent of the Internet dramatically changed the way information was exchanged. Connecting computers, then computing devices, together created a new informational paradigm. The automation of information broadcast (the data servers) allowed an incredible access to information: the physical barriers that used to hamper the diffusion of information fell, only limited by intellectual property issues. In addition,

---

[3] Simon Singh, *The Code Book: the Secret History of Codes and Code-breaking* (London, UK: Fourth Estate, 2000); Bradford J. Shwedo, *XIX Tactical Air Command and ULTRA: Patton's Force Enhancers in the 1944 Campaign in France*, CADRE Paper no. 10 (Maxwell Air Force Base, AL: Air University Press, 2001), 13.
[4] "The Impact of WWI on the Course of American Radio History," http://www.academia.edu/937415/The_Impact_of_WWI_on_the_Course_of_American_Radio_History (accessed February 20, 2013).

the integration of computing devices with automated systems enabled increasingly sophisticated computing systems.

Another phenomenon added relevance to the concept of a cyberspace as an integrated informational environment. While the Internet was initially dedicated to computers only, recent protocols standardization increasingly broadened the perimeter of cyberspace. Indeed, computers, smartphones, and smart televisions are interconnected and exchange increasing amounts of data. Computer networks, satellite data links, or cellular phone networks present similar characteristics and stakes that political actors must address globally.

A recurrent debate about cyberspace today concerns its legitimacy as a warfighting domain. To share in the debate, it is first necessary to characterize what is meant by a domain or medium, and to highlight the supplementary characteristics that define a domain. A study of existing physical domains, their role in social activities and how their definition influences international relations and military theories will provide valuable insight on the requirements for a useful definition of cyberspace

Medium and Domain Characterized

The classification of cyberspace as a medium, a domain, or something else has raised heated debates that are not devoid of organizational stakes. This section aims to contribute to the debate. An accurate characterization of mediums and domains will serve as a basis to compare the constituting elements of a medium and a domain to that

of cyberspace. While a medium usually describes a homogeneous environment, a warfighting domain is a socially constructed entity, usually leaning on a medium. Thus, a domain is characterized by relative continuity and delimitability, by strategic significance, and by the development of specific means to explore, exploit, and control it.

According to the Merriam-Webster dictionary, a medium is a distinct "environment in which something may function or flourish."[5] The definition of a domain is hardly more specific: it is "a territory over which dominion is exercised," "a region distinctly marked by physical features," or "a sphere of knowledge, influence or activity."[6] These definitions are too vague for a characterization of cyberspace. Indeed, two different concepts underpin physical domains and mediums. There are first *natural* environments, in which activities may take place. They do not depend on human activities to exist, they simply are. In addition, human activities, among which military ones, categorize portions of the environment following the nature of activities that take place in it, or the *technology* employed. I will take the stance to call *medium* the first concept, and *domain* the second one.

A medium is usually a relatively homogeneous environment. For instance, the air forms an uninterrupted environment starting from the

---

[5] "Merriam-Webster's Collegiate Dictionary" (Springfield, MA: Merriam-Webster, Inc., 2008), 771.
[6] "Merriam-Webster's Collegiate Dictionary," 370.

ground upwards. For land or for the seas, the continuity is more relative: there may be some level of discontinuity, like continents for land or closed seas. Nevertheless, these discontinuities resort to the medium geography.

In addition, natural mediums show common environmental characteristics and usually host specifics ecosystems.[7] On the contrary, domains owe their characterization to social organization. Moreover, domains have strategic and political significance. For instance, the development of maritime technology initiated the Chinese expansion from 1000 onward.[8] As this paper is focused on strategy, I will characterize domains according to their use in international politics and by military organizations.

In international relations, domains are referred to in relation to power. Naval strategist Alfred T. Mahan showed that throughout history, the maritime medium had created new economic opportunity, which in turn fostered the development of the means to protect a country's interests in the medium.[9] Thus economic interests and military means have developed in parallel and support each other's growth. Therefore, discussing sea power as a whole is relevant, since neither economic power stemming from sea trade nor military means to control the sea can

[7] The French Encyclopedia Larousse defines a medium as "the material space in which a body is placed." "Larousse du XXe Siecle vol.4", ed. Larousse (Paris, 1928), 772.
[8] William H. McNeill, *The Pursuit of Power: Technology, Armed Force, and Society Since A.d. 1000* (Chicago, IL: University of Chicago Press, 1984), 50.
[9] A. T Mahan, *Mahan on Naval Strategy: Selections from the Writings of Rear Admiral Alfred Thayer Mahan* (Annapolis, MD: Naval Institute Press, 1991), 27–29.

be addressed in isolation. Similarly, airpower developed more consciously as a means of coercion—to some extent, its military development preceded its economic use.[10] Nevertheless, Giulio Douhet and Billy Mitchell, early advocates of airpower, emphasized the importance of a strong air-minded economy in generating powerful air forces.[11] Domains are mediums prone to the exercise of power in all their dimensions.[12]

Domains show other common characteristics. The underlying medium must be specific enough to require technological and operational expertise. Thus, sea and air have required the development of ships, techniques of navigation, and motivated specific military strategies. An interesting example is that of space. Despite a lack of clear demarcation with the air, outer space requires distinct access and control assets, which advocates for a separate space domain.

The early development of airpower provides another interesting example. Its strategic interest initially rested in military, more than economic, power. Nevertheless, as Billy Mitchell advocated shortly after,

---

[10] The early developments of aviation was largely financed by the military. Clement Ader's "avions" were subsidized by the French Army since 1892 (16), and aviation played a significant role as early as WW1. Commercial aviation hardly developed before the end of WW1. Edouard Chemel, *Chronique de l'aviation.* (Paris: Éditions Chronique Acropole, 1991), 16.

[11] William Mitchell, *Winged Defense the Development and Possibilities of Modern Air Power--Economic and Military* (Tuscaloosa, AL: University of Alabama Press, 2009); Giulio Douhet, *The Command of the Air*, Fire Ant Books (Tuscaloosa, AL: University of Alabama Press, 1998).

[12] David Baldwin categorized states power according to their effects in economy, diplomacy, military and in the informational area. David A. Baldwin, *Economic Statecraft* (Princeton, NJ: Princeton University Press, 1985), 13.

civil aviation offers tremendous opportunities and supports the building of national airpower.[13]

As an important mode of social interaction, warfighting contributes to the strategic significance of a domain. Military strategy professor Everett Dolman offered valuable selection criteria for military domains, stemming from their utility in strategy. Operational strategies, he argued, must both be supportive to the global military strategy and yet unique to other operational strategies.[14] The discriminating factor he offered rests therefore on the form of military power. These forms depend on the ability to exercise violence from a given medium.[15] Therefore, military domains are mediums from which it is possible to exercise some kind of violence in pursuance of political effects.

This framework is insufficient to characterize domains at large. Indeed, although an important one, the exertion of violence is but a component of political and military importance.

For instance, legal restrictions forbid the exertion of some types of violence from space. Yet, even a non-weaponized space produces political

---

[13] Mitchell, *Winged Defense the Development and Possibilities of Modern Air Power--Economic and Military*, 98.
[14] Everett C Dolman, *Pure Strategy: Power and Principle in the Space and Information Age* (New York: Frank Cass, 2005), 27.
[15] In *Pure strategy*, 30–31, Dr. Dolman did not actually explain why the different forms of power coincided with physical mediums. His analysis supposes a natural and obvious delimitation of the domains, which is far from evident for cyberspace.

effects, for instance with means of observation or surveillance.[16] Space has critically improved the application of force from the air, land, or sea. Therefore, even without a prospect of exertion of violence from space, a strategy of control of space makes sense to gain a decisive advantage in the exertion of violence from other mediums. Consequently, a more exact statement of the definition of a domain from a military standpoint would be a medium whose control has a decisive impact on the pursuance of political objectives.

To summarize, domains are mediums (or portions thereof) of strategic significance requiring the development of specific assets to explore, exploit, and control them. They are essentially social constructs.

An important distinction must be made between the domain and the activities that take place within it. A domain is distinct from the assets that constitute the expression of power in the domain, which, in turn is distinct from the instruments of power that develop within this domain. For instance, air as a medium is a physical space filled with gas molecules. It can be considered as a domain because taking advantage of its benefits has required the development of specific technology and expertise, and it is economically and militarily important. Now, airpower is made of a variety of assets, some of them not resting in the air at all: aircraft industry, military means, and presence in international

[16] The international disagreement over the existence of weapons of mass destruction in Iraq (2003) provides a powerful example of the critical political value of space-based assets.

organization are all attributes of airpower. Finally, airpower contributes to military, economic, diplomatic, and informational instruments of power but each of these instruments of power operates across existing domains.

To be eligible as a domain, cyberspace should show the physical characteristics of the medium and the social characteristics of a domain. These criteria will inspire its definition and the elements I may consider part of, or external to it.

Cyberspace Defined

To discuss the nature of cyberspace, it must be accurately circumscribed first. A definition of cyberspace must account for its constituting parts but also fit with other aspects of international politics and military organizations. Therefore, in order to define it in a similar fashion to traditional domains and allow its conceptual integration with the traditional instruments of power, I will limit my definition of cyberspace to the tangible components that support information exchanges.

Defining the exact contours of a medium can seem unnecessary for a physical one, but cyberspace encompasses or interacts with several

physical and virtual, technical and sociological dimensions.[17] Including or excluding a component has tremendous consequences for the conceptualization of strategies and organizations designed to operate within cyberspace. Indeed, "What I decide to include or exclude from cyberspace has significant implications for the operations of power, as it determines the purview of cyberspace strategies and the operations of cyberpower."[18]

In addition, to be useful, a definition of cyberspace must fit within the existing body of theories and underlying set of definitions. Political scientist David Baldwin offered preferred criteria for the selection of taxonomy.[19] By analogy, our definition must be in "conformity with scientific canons requiring parallel categories to be mutually exclusive and exhaustive of all cases," and "avoidance of unnecessary departures from common usage."[20] To put it in mathematical terms, the set of mediums and that of domains must constitute a partition of the physical environment.[21]

---

[17] Franklin D. Kramer, "Cyberpower and National Security: Policy Recommendations for a Strategic Framework," in *Cyberpower and National Security*, ed. Franklin D. Kramer, Stuart H Starr, and Larry K Wentz (Washington, DC: Potomac Books, 2009), 4.
[18] David J. Betz and Tim Stevens, *Cyberspace and the State: Toward a Strategy for Cyber-power*, 424 (London, UK: The International Institute for Strategic Studies, 2011), 36.
[19] In *Economic Statecraft*, 12, Baldwin classified the different techniques of statecraft. He identified several criteria that added to the utility of a specific taxonomy.
[20] Baldwin, *Economic Statecraft*, 12.
[21] I am using "partition" and "universe" in a mathematical sense here (theory of ensembles). It is a certain set, fixed within the framework of a given fundamental theory and containing as members all objects considered in this theory. Several sets form a partition of a universe if they are mutually exclusive and globally inclusive of the universe. For more details, see Universe. B. Pareigis (originator), *Encyclopedia of*

Intelligence professor Daniel Kuehl reviewed several tentative definitions for cyberspace.[22] Many of them are strongly influenced by organizational concerns.[23] Nevertheless, although definitions inspire organizations, existing organizations of cyber-activities should not influence a definition of cyberspace. Doing so would simply perpetuate the existing paradigm, and might hamper a more effective social organization of cyberspace. The definition selected will underpin an analysis of cyberpower in international relations, as well as the characterization of a military operational domain. Accordingly, it must be able to integrate with existing bodies of theories, but shall not presuppose a specific organization.

Cyberspace, taken globally, is an environment within which digital communications take place. Its primary purpose is informational: cyberspace creates, processes, and exchanges information.[24] Such exchange can involve sensible or technical data and include machine-to-

---

Mathematics. http://www.encyclopediaofmath.org/index.php?title=Universe&oldid=11866; Partition. M.I. Voitsekhovskii (originator), *Encyclopedia of Mathematics*. http://www.encyclopediaofmath.org/index.php?title=Partition&oldid=16216 (accessed 20 April 2013).

[22] Daniel Kuehl, "From Cyberspace to Cyberpower: Defining the Problem," in *Cyberpower and National Security*, ed. Franklin D. Kramer, Stuart H. Starr, and Larry Wentz (Dulles, VA: Potomac Books, Inc., 2009), 24–42.

[23] Thus, the National Security Presidential Directive issued in 2008 defined cyberspace as "interdependent network of information technology infrastructures, and includes the Internet, telecommunications networks, computer systems, and embedded processors and controllers in critical industries." It is obvious here that such a definition seeks to encompass the elements of cyberspace that are relevant to national security. Kuehl, "From Cyberspace to Cyberpower: Defining the Problem," 27.

[24] Kuehl, "From Cyberspace to Cyberpower: Defining the Problem," 26.

machine communication or require human intervention.[25] Each definition Kuehl listed encompasses or alludes to the following strata.[26] The physical implementation of cyberspace is composed of computing devices and the means for networking. This stratum includes computers, smartphones, and other smart devices, but also networking assets: routers and repeater satellites, wires, and the electromagnetic spectrum used to transmit data.[27] The upper stratum, the syntactic layer, "consists of the formatting of information and the rules that instruct and control the information systems that make up cyberspace."[28] This level encompasses the software as well as the technical data circulating within a network. Finally, "the semantic layer consists of information useful and comprehensible to human users."[29] It is the useful information conveyed within cyberspace, intended for human consumption and understanding.

Whether a definition of cyberspace should include a semantic layer is debatable. On the one hand, cyberspace is characterized as a medium in which information *flow*s. The cognitive component has been a critical

---

[25] Indeed, even some disconnected networks can communicate. The exchange of information through removable media is still a connection, for instance. Therefore, given that a system without informational exchange at all would be of very limited interest, I can suppose that *any* network of communicating devices can be part of cyberspace.
[26] Kuehl, "From Cyberspace to Cyberpower: Defining the Problem," 26–27.
[27] For this layer, Sheldon added the electromagnetic spectrum used for wireless communications to Martin Libicki's description of the physical layer. This improvement is consistent with Sheldon's taxonomy, since upper layers take advantage of lower strata's services regardless of the technologies used to transmit information. John B Sheldon, "Toward a Theory of Cyberpower," in *Cyberspace and National Security*, ed. Derek S. Reveron (Washington, DC: Georgetown University Press, 2012), 213; Martin C. Libicki, *Conquest in Cyberspace: National Security and Information Warfare* (New York: Cambridge University Press, 2007), 8.
[28] Sheldon, "Toward a Theory of Cyberpower," 213–214.
[29] Sheldon, "Toward a Theory of Cyberpower," 214.

motive for the development of cyberspace.[30] On the other hand, including a cognitive dimension to cyberspace poses a problem of discrimination with other mediums, as well as between this medium and the informational instrument of statecraft. Indeed, information warfare ranges across the military domains. Creating a conceptual discontinuity between cyberspace and other military domains would harm information-related doctrine. Similarly, since cyberpower operates across the whole range of diplomatic, informational, military, and economic (DIME) instruments of statecraft, cyberspace is better defined as a medium that does not include the cognitive and social interactions that take place within it.[31] Indeed, the model that has prevailed describes different (physical) domains, within which the whole range of the instruments of statecraft can operate.[32]

Some documents refer to cyberspace as a subset of the informational domain.[33] In this analysis, it is inaccurate to refer to an informational *domain*. Indeed, information flows in many mediums, wherever there is social interaction. Military use of information, for

---

[30] For instance, Lonsdale implicitly encompassed the semantic layer, considering cyberspace within the wider issue of information warfare. Lonsdale, *The Nature of War in the Information Age*, 2004, 10.
[31] For a discussion on the instruments of statecraft, see Baldwin, *Economic Statecraft*, 8–15.
[32] Baldwin, *Economic statecraft.* In this seminal work, Baldwin described the diplomatic, economic, military and propaganda instruments of statecraft. Cyberspace cannot be another instrument of statecraft, because it produces political effects across the categories aforementioned. It can be better thought of as a medium, like the sea, or the air, within which diplomatic, military, informational and economic activities take place.
[33] For instance, Lonsdale, *The Nature of War in the Information Age*, 2004.

instance, plays an important role in counterinsurgency in land warfare. Therefore, considering such a domain does not allow a segregation of the domains. Moreover, it blurs the distinction between communication medium and communicated items. Information warfare may be a subset of a general strategy, and it would operate across several domains.[34]

The integration of a syntactic layer within cyberspace is not self-evident either. On the one hand, if I exclude information flows from the semantic layer, why encompass information from the syntactic layer? On the other hand, technical data and infrastructures are essential to the functioning of cyberspace. It is an internal characteristic that determines its geography, its behavior. Disregarding it would hamper comprehensive systemic approaches to cyberspace. In addition, the information from the syntactic layer is specific to cyberspace and does not permeate other domains.

Therefore, I will use the definition of cyberspace from the US National Military Strategy for Cyberspace Operations: cyberspace is "a domain characterized by the use of electronics and the electromagnetic spectrum to store, modify and exchange information via networked systems and physical infrastructure."[35] This definition of cyberspace is

---

[34] See for instance Joint Publication Document, "JP3.13 Joint Doctrine for Information Operations," November 27, 2012, i.
[35] Kuehl, "From Cyberspace to Cyberpower: Defining the Problem," 27.

not only useful for a military strategy;[36] since it also encompasses the infrastructures that support the cyber-economy or the vectors of informational influence, it is equally useful in support of other human activities.[37]

Cyberspace: New Frontier, New Domain

According to the constituting characteristics of mediums and domains offered earlier, the proffered definition of cyberspace describes a domain. Indeed, cyberspace is a medium distinct from other ones (it can be segregated), it is the support for informational ecosystems and for social interactions, and its integrations into the set of other mediums forms a partition of the geopolitical universe. Finally, its strategic significance and the specific assets required to operate within it legitimize it as a domain.

First, cyberspace can be thought of as a whole. Although made of distinct entities spread on the ground (computing and networking hardware), under the seas (the transcontinental wires), in the air (electromagnetic wireless connection), and even in space (repeater satellites), information roams across the whole spectrum of cyberspace

---

[36] It is important to notice that the National Military Strategy for Cyberspace draws a clear distinction between cyber operation and information operations. Air Force Doctrine Document, "AFDD 3-12, Cyberspace Operations," July 15, 2010, 2.
[37] Cyberpower "is not created simply to exist, but rather to support the attainment of larger objectives across the elements of national power--political, diplomatic, informational, military, and economic." Betz and Stevens, *Cyberspace and the State*, 44.

elements constantly.[38] It does not mean that there is no cyberspace geography, though. Cyberspace is everything but even.[39] Its functional homogeneity stems from the convergence of digital communication protocols, allowing semantic and syntactic information to flow throughout.

Second, cyberspace as a medium is distinct from others. For sure, its physical elements rest on land, under the seas, in space, and even in the air. Nevertheless, these elements are distinct from the aforementioned mediums by their purpose. It is their functional integration that distinguishes those assets from their physical implantation.

Cyberspace can therefore be thought of as a medium. In addition, it also includes the characteristics of a domain. First, cyberspace is the support of distinct social activities. Thus, the European Union white paper entitled "Growth, Competitiveness, Employment: the Challenges and Way Forward into the 21st Century" emphasized the emergence of an

---

[38] Luciano Floridi, "The Future Development of the Information Society," *Jahrbuch Der Akademie Der Wissenschaften in Göttingen* (2007): 175–187. In this article, Floridi, explained that the ability of digital devices to communicate "effortlessly and seamlessly" has almost suppressed the friction in infosphères. Consequently, the cognitive border between physical and virtual will tend to fade (180-181).

[39] The geography of cyberspace can be approached under a technical perspective. A review of several geographical models that apply to this dimension of cyberspace can be found in Guoray Cai, Stephen Hirtle, and James Williams, "Mapping the Geography of Cyberspace Using Telecommunications Infrastructure Information," *TeleGeo* (1999): 6–7; Besides, a sociological approach to the geography of cyberspace is offered by Steve Mizrach, *Lost in Cyberspace: a Cultural Geography of Cyberspace* (Steve Mizrach, 1996), http://www2.fiu.edu/~mizrachs/lost-in-cyberspace.html (accessed 17 March 2013).

information society in which a significant portion of economic and social interaction took place.[40]

Therefore, the strategic significance of cyberspace stems partially from its social importance. Cyberspace has revolutionized many aspects of human life, and it has shaped social interactions, economic exchanges, and wealth production. Consequently, its political and military importance has increased accordingly.[41]

The steady growth of online commerce is but the tip of the iceberg. Indeed, cyberspace has vested many other aspects of the world's economy. To illustrate the extent of this revolution, I will take two examples. First, the sector of logistics deserves particular scrutiny for its implication in most economic sectors. "Logistics industries have become especially significant in the light of broader changes: new production methods, involving increased flexibility; changing relationships between customers and suppliers; increasing use of just-in-time procurement and delivery systems; and increasing geographical complexity and extent of production networks."[42]

---

[40] *Growth, Competitiveness, Employment: The Challenges and Ways Forward into the 21st Century: White Paper*, Bulletin of the European Communities. Supplement 6/93 (Luxembourg: Office for Official Publications of the European Communities; UNIPUB, distributor, 1993), 92–94.
[41] Antoine Bousquet highlighted the connection between the social organization for the production of goods, the social organizations, and the focus of destructive forces. Antoine Bousquet, *The Scientific Way of Warfare: Order and Chaos on the Battlefields of Modernity* (New York: Columbia University Press, 2009), 18.
[42] Peter Dicken, *Global Shift: Mapping the Changing Contours of the World Economy* (New York: Guilford Press, 2011), 400.

It is important to notice that the advent of cyberspace has essentially made *all* these improvements possible. Indeed, among the technological innovations that economist Peter Dicken has identified as instrumental, I can find: electronic data interchange (the information technology (IT) systems allowing connection of all the levels of the supply chain, identifying products specifications, purchase order, invoices, status of the transaction, stocks, and the like); bar codes and radio-frequency identification devices (RFID); and distribution centers.[43] All these innovations are cyberspace-related. In addition, e-commerce also brought significant changes in relations between businesses and customers.[44]

Another industrial sector worth of scrutiny is that of the automobile. Its significance lies in its scale and in its linkages to many other manufacturing industries and services. Approximately eight million people are employed directly in automobile production. If I add in those involved in selling and servicing vehicles, I reach a total of up to 20 million workers.[45] Moreover, automotive products are responsible for almost half the world's oil consumption, and their manufacture uses up nearly half the world's output of rubber, 25% of its glass, and 15% of its

---

[43] Dicken, *Global Shift*, 404–406.
[44] See Dicken, *Global Shift* for more details on business-to-business, business-to-consumer, consumer-to-business and consumer-to-consumer models.
[45] Dicken, *Global Shift*, 332.

steel.[46] On top of the revolution of logistics that deeply restructured the sector's processes and industrial model, the automobile industry has dramatically shifted from mass production to lean production.[47] Because of the level of automation, the high level of integration of manufacturers and suppliers, the whole sector is highly cyber-dependent.

The advent of cyberspace has had tremendous impact on social life as well. Thus, anthropologist Scott Atran extended the notion of the tribe to cyberspace. "This broader idea of tribe refers to a group of interlinked communities that largely share a common cultural sense of themselves, and which imagine and believe themselves to be part of one big family and home. Today the imagined community, as political scientist Benedict Anderson once referred to the notion of the nation, extends from city neighborhoods to cyberspace."[48]

Moreover, besides technological evolutions, the evolutions of war have fit closely those of human activities.[49] Accordingly, the political and military importance of cyberspace grows according to two factors. Cyberspace, as a force enabler, facilitates the exertion of physical violence. Therefore the control of this medium for military purposes is a precondition to the effective use of force. In addition, cyberspace also offers autonomous means of influence and coercion. Thus, cyberspace is

---

[46] Dicken, *Global Shift*, 332.
[47] Dicken, *Global Shift*, 339.
[48] Scott Atran, *Talking to the Enemy: Faith, Brotherhood, and the (un)making of Terrorists* (New York: Ecco Press, 2010), 9.
[49] Bousquet, *The Scientific Way of Warfare*, 17–18.

a privileged support of information, and it is therefore a natural battleground for ideas. Controlling cyberspace would therefore grant a decisive advantage in this area. Moreover, many systems providing critical needs can be reached and attacked *from* cyberspace. Violence can therefore be exerted from this medium. Finally, data constitute increasingly critical assets on their own. Using coercion *within* cyberspace, threatening an enemy's cyber-infrastructure becomes possible as well.

The virtual nature of cyberspace has challenged the basis of international law, blurred national borders, and complicated the distinction between state and non-state actors since both can acquire comparable capabilities and wage almost symmetric conflicts. Consequently, strategists struggle to apply the canons of the discipline to this unsettling domain.

Cyber-Challenges to Strategic Wisdom

Although cyberspace possesses the attributes of a domain, it also has distinct specificities that suggest a thorough review of the classical theories of war and of the mechanisms of international politics.

International relations are based on social interactions. One would think that this does not significantly change, but, as I showed, cyberspace modified some parameters of social interactions. Its borderless nature has, in conjunction with easier international travels, created transnational communities. The strength of the cohesive links of

such communities is variable, but this emerging phenomenon, part of the greater challenge of globalization, is a first challenge to theories using states and international organizations as sole IR unit.

Virtualization—the fact that assets and actions may not be associated to a specific actor under a specific authority—also challenges legal norms. Indeed, international law essentially codifies the settlement of disputes between states, while domestic laws manage deviant behavior within their territorial area. Now, cyberspace blurred this clear distinction and poses several legal challenges. First, an attack can originate from country A and exploit vulnerabilities in country B to attack country C. Criminals, individuals or organizations, can take advantage of the lack of legal homogeneity, for instance regarding servers logging, to conceal their attacks and escape prosecution. In addition, the motivation of the individual determines the body of law applying to the case, which is another source of indeterminacy.[50]

The global commons is another paradox of cyberspace. Indeed, cyberspace is rooted on physical implantations that technically belong to states. Yet, some infrastructures of cyberspace may very well become a global common, like international waters. The domain name service (DNS) of the Internet offers a relevant example. The DNS is the service

---

[50] David P. Fidler, "Inter Arm Silent Reges Redux? The Law of Armed Conflict and Cyber Conflict," in *Cyberspace and National Security*, ed. Derek S. Reveron, Georgetown University Press (Wahington, DC, 2012), 71–87. The same attack can be state led and therefore addressed to by the law of armed conflict (LOAC), motivated by criminal activities (which involves both domestic law and international police cooperation.

translating IP addresses (32 bits or 128 bits number) into comprehensible names (www.blahblah.org). It is a hierarchical structure in which root servers are at the top of the hierarchy, and national, commercial, and other organizational domains are directly under these root servers. Although an individual root server is under the objective authority of the hosting state, the service itself, including the database of national and organizational name domains could be beyond any state's authority, since the modification of any individual server would not threaten the DNS infrastructure, other servers being able to fulfill the same service. Thus, some infrastructures and assets of cyberspace can be virtual, too.

Finally, conflict in cyberspace challenges classical theories of war in two ways. First they blur the essential notions underpinning strategy. Cyber-attacks can strike anywhere from anywhere, abolishing the notion of distance. In addition, the effects of cyber-attacks can be instantaneous, leaving no room for adaptation and interaction, which is a fundamental parameter of strategy. Finally, cyber-forces and masses are still to be defined. Indeed, a single person can design attacks that may threaten a significantly larger organization.

Second, the theorizing process draws upon a set of assumptions and a simplified model of reality. Thus, current international politics and military theories are underpinned by characteristics that do not apply simply in cyberspace. A clarification of these principles and their

underpinnings is therefore necessary to transpose the logic of these theories into cyberspace.

Chapter 2

Force in International Politics

Cyberspace plays a growing role in economic and social life, but its role in international politics at large, and in political disputes in particular, remains largely misunderstood. War being "politics by other means," any relevant cyber-strategy must clearly clarify the mechanisms that transform the use of violence from cyberspace into political effects.[1] Therefore, as a preamble to cyberspace strategy, I must analyze the political instrumentality of violence in international relations in order to grasp the purposes of cyber-strategy, the range of possible actions and the limits of cyberspace in conflict resolution.

It is argued here that violence produces political effects because it influences the bargaining calculation of a competitor, either by demonstrating the unlikeliness of enemy success, or by raising the price of opposing friendly interests. The role of military action therefore lies in distorting the enemy's perceptions, more than merely establishing a situation that will remain after the conflict.

To come to that conclusion, it is necessary to describe the actors of international relations. Initially the only actors of international politics, states, have gradually met the competition of other, non-state, political

---

[1] Carl von Clausewitz, *On War*, trans. and ed. Michael Howard and Peter Paret (Princeton, NJ: Princeton University Press, 1984), 80.

actors. Their interaction may end up in the use of violence for a variety of reasons. Nevertheless, the use of violence never completely obliterates other political interactions. More than a brutal application of force, wars are a bargaining tool. The mechanisms of coercion, therefore, explain not only specific coercive strategy but more generally wars' termination. The last two sections develop the logic of coercion and its limits.

Actors of International Relations

Initially built around the supremacy of states, the ecosystem of political entities populating the international arena is now far more diverse. Nevertheless, states still possess the unequaled power to focus the might of a whole society as well as a legal supremacy.

The state has gradually become the most powerful social organization, primarily because it was able to concentrate large amounts of power to defend itself and ensure its internal cohesion. Indeed, it is possible to observe a social organization owning the modern function of a state as early as the fourth millennium BC in Mesopotamia. This organization, made possible by the use of writing (for the diffusion of law, thereby ensuring internal coherence) and agriculture (entailing settlement and creating the need for permanent defense), proved more effective and gradually dominated social organizations.[2]

---

[2] Anthony Giddens, *A Contemporary Critique of Historical Materialism. Vol. 2, The Nation-state and Violence* (Los Angeles, CA: University of California Press, 1987), see Chapter 2.

International law formalized the preeminence of states and developed a clear separation between individuals and states. The object of international law is only states—with the notable addition of international institutions, individuals' rights are defined by domestic law.[3] However, several political actors have emerged and now challenge the supremacy of states in several domains. Historically, large companies have been the first non-state actors to gather political significance at the international level. Thus, British and French overseas trade companies fought relentless wars to increase their hold on oversea markets. In some instances, they strained the relations between both countries.[4]

International political organizations are another kind of non-state actor. Although they usually gather limited power on their own, their power stems from their members, whether states, individuals, companies or a mix thereof. The political intent of international political organizations heavily depends on their status, their mission, and their members' interests. Finally, informal networks bound by transnational ideologies have spread since the twentieth century. These political groups

---

[3] Some norms of international law suggest minimal rights to individuals, especially the human rights treaties. Nevertheless, the *object* of treaties remains states that have to comply with this treaty. Similarly, the International criminal court does address individual crimes, but only either those of citizens of signatory states, or those committed in a signatory state, or crimes submitted to the security council of the united nations. *Rome Statute of the International Criminal Court*. http://untreaty.un.org/cod/icc/statute/99_corr/cstatute.htm (accessed 19 May 2013).

[4] For instance, the French Compagnies des Indes were oversea trade companies that had a tremendous political importance. They were to some extent an instrument of states politics, but they also gained political power on their own, until they threatened the state and were dismantled. Archives Nationales, "Compagnie Des Indes," accessed May 20, 2013, http://www.memoiredeshommes.sga.defense.gouv.fr/indes/.

without a legal existence count many outlawed groups such as Al Qaeda, the Red Factions, or Euskadi Ta Askatasuna (Basque Homeland and Freedom—ETA). They threaten the interests of states and regularly use violence to fulfill their political objectives, hence their banishment and qualification as terrorist groups. Nevertheless, they pursue a political aim, possess political power, and therefore are relevant political units to consider.

Nevertheless, working states still hold an uncontested supremacy in a variety of critical areas. The power of non-state actors is limited to that which states grant them.[5] First, states have legal supremacy over the territory under their control and in international politics. Thus international companies have head offices and are required to abide by domestic and international laws. In addition, the level of physical power states can extract from societies can seldom be matched by non-state organizations. For instance, military mobilization and tax collection provide the state with unequaled ability to marshal the resources of a society.

War, Violence and Politics

Violence appears amongst the range of interaction between political actors. It is one way for political actors to relieve a political

---

[5] Thus, transnational movements take advantage of states either unwillingness or inability to fight them. Therefore, they are either a tacit instrument of state politics or a symptom of the disaggregation of some states.

tension. When used, its intensity varies from isolated blows to total engagement of resources.

Indeed, political entities interact in a variety of ways, and war is one of them. In his extensive study of war, political scientist Quincy Wright characterized the latter phenomenon as the manifestation of a political tension. War, he concluded, stems from a major change in one of the following parameters: technology, particularly as it applies to military matters; law, particularly as it pertains to war and its initiation; social organization, particularly in regard to such general-purpose political units as tribes, nations, empires, and international organizations; and the distribution of opinions and attitudes concerning basic values.[6]

This categorization encompasses two distinct phenomena. First, it acknowledges the role of ideological values as a potential motive for war. In addition, economy has been a powerful motive as well, although its effectiveness "is dubious at best."[7] Finally, Wright added, the political motives of war mostly regard increase or assertion of power.[8]

War is a specific case of the use of violence for political purposes. Historically a legally and socially distinct type of political interaction, the spectrum of violence has significantly broadened since WWII. Thus, states use terrorist organizations or covert action to destabilize a

---

[6] Quincy Wright, *A Study of War* (Chicago, IL: University of Chicago Press, 1965), 1284.
[7] Wright, *A Study of War*, 281.
[8] Wright, *A Study of War*, 278.

competitor in peacetime; they organize isolated retaliatory strikes or lead limited military operations. The use of violence in politics requires scrutiny because it describes not only the purpose of war but more broadly its instrumentality.

Instrumentality of Violence

War is the purest expression of violence in international relations. Yet, despite episodes of the brute imposition of physical superiority, war almost inevitably ends up as a diplomatic bargain. Therefore, military effectiveness resides in its promises more than in its tangible achievements.

Studying the character of the diplomacy of violence, political scientist Thomas Schelling made a clear distinction between two radically different uses of violence for political purposes. *Brute force*, he argued, is used when "some things a country wants it can take, and some things it has it can keep, by sheer strength, skills and ingenuity."[9] "With enough force, a country may not need to bargain."[10] On the opposite, coercion involves an interaction, the anticipation of pain by the enemy that provides a bargaining advantage.[11]

---

[9] Thomas C. Schelling, *Arms and Influence* (New Haven, CT: Yale University Press, 2008), 1.
[10] Schelling, *Arms and Influence*, 2008, 1.
[11] Schelling, *Arms and Influence*, 2008, 2.

Nevertheless, there have been very few occurrences of use of brute force without any bargaining throughout history.[12] Even once the enemy army has been defeated, surrender and armistice negotiations take place. The victor could invade the whole territory and submit the populations, but this seldom—if ever—occurs. Undeniably, as Clausewitz emphasized, the destruction of the enemy's armed forces makes him vulnerable to destruction and provides the victor with tremendous bargaining leverage. However, Clausewitz acknowledged, it is not war itself but the political bargaining that ensues that defines the outcomes of a war.[13] For instance, the vanquished still has the opportunity to pursue the fight and inflict more pain on the enemy, notably through insurrections. Thus, despite the decisive victory of German troops over the French army, Adolf Hitler did not choose to push his advantage and seize the whole mainland. Arguably, such supplementary effort would have diverted much needed military resources, for a land that was not part of the German envisioned *Lebensraum*, nor of strategic significance.[14] In addition, imposing too harsh surrender conditions could have resumed the fighting, whether from the homeland or from northern Africa. From the French prospective, the dominant priority "favored an immediate

---

[12] Even for the Japanese surrender in 1945, negotiations took place despite Roosevelt's initial claim that the USA would require unconditional surrender. Although the text refers to unconditional surrender, preliminary negotiations took place. Herman S Wolk, *Cataclysm: General Hap Arnold and the Defeat of Japan* (Denton, TX: University of North Texas Press, 2010), 192–194.
[13] Clausewitz, *On War*, 80.
[14] J. Adam Tooze, *The Wages of Destruction: The Making and Breaking of the Nazi Economy* (New York: Penguin USA, 2008), 8–9.

ceasefire to save France from further losses."[15] Nonetheless, General Charles de Gaulle advocated a competing alternative of resisting the Germans, if necessary from outside metropolitan France.[16]

Therefore, the conflict termination process (i.e. the *raison d'être* of strategy) systematically ends up as a bargaining process. Each side has to agree on the final terms of the settlement: the holding of territory by a foreign force does not necessarily mean its eventual annexing. The value of military (or violent) operations, therefore, lies in the bargaining advantage it may provide to the conflict termination negotiations.[17] "If I keep in mind that war springs from some political purpose, it is natural that the prime cause of its existence will remain the supreme consideration in conducting it. That, however, does not imply that the political aim is a tyrant. It must adapt itself to chosen means, a process that can radically change it."[18]

"Diplomacy," Thomas Schelling argued, "is bargaining; it seeks outcomes that, though not ideal for either party, are better for both than some of the alternatives … There must be some common interest, if only

---

[15] Richard Holmes, *The Oxford Companion to Military History* (Prato, IT: Oxford University Press, 2004), 316.
[16] This clash eventually led to the divorce between the Vichy regime, that abode by the German condition and cooperated with it, and the *France Libre* (Free France) government, that settled in London and organized both the resistance in France and the Free French Forces, that resumed the fight from Northern Africa and Great Britain. Holmes, *The Oxford Companion to Military History*, 327.
[17] For a god description of the tensions accompanying the war termination process, see, for instance, Fred Charles Iklé, *Every War Must End* (New York: Columbia University Press, 2005), chap. 4.
[18] Clausewitz, *On War*, 87.

in the avoidance of mutual damage, and an awareness of the need to make the other party prefer an outcome acceptable to oneself."[19]

I can therefore conclude that, although conflicts can have episodes of brute violence, conflict resolution usually involves negotiation, which is grounded on the prospects of gain or losses of both belligerents. The purpose of military action, therefore, is to generate such a situation that the achievement of friendly objectives appears unambiguous to the enemy.[20]

Although scholars have often studied coercion as a specific political and military option, the logic it describes transcends this narrow application. Of course, the advent of ubiquitous weapons—weapons that essentially go round enemy defenses and can strike any portion of the enemy state—makes coercive strategies attractive.[21] But more generally, coercion tends to systematically become a component of military action. Moreover, its underpinnings, the way violence modifies enemy cost-benefit analysis, apply to any conflict bargaining situation.

Incentives and Punishment: the Logic of Coercion

Chinese strategist Li Bingyan offered an interesting perspective. He contended that "The best strategy tries to entice the opponent to adopt a

---

[19] Thomas C Schelling, *Arms and Influence* (New Haven, Conn.; London: Yale University Press, 2008), 1.
[20] André Beaufre, *Introduction à la Stratégie* (Paris: Pluriel, 2012), 34.
[21] Robert Anthony Pape, *Bombing to Win: Air Power and Coercion in War* (Ithaca, NY: Cornell University Press, 1996), 2.

strategy that will lead China to the greatest gains."[22] Similarly, the logic of coercion is entirely focused on the enemy's risk-benefits calculations. Whether raising the cost of unwanted strategies or undermining the perceived chances of success, it aims at discrediting enemy strategic options that would harm friendly interests to foster ones that are more in line with friendly priorities.

Thomas Schelling made an important contribution to the understanding of the phenomenon. In *Arms and Influence*, he distinguished brute force from coercion that involves an enemy's perception of the outcomes of a prolonged conflict. Coercion acknowledges the enemy's free will. Therefore, violence is not directly geared towards the objective itself but instead towards the enemy will and interest to deny it.[23]

To achieve this effect, the coercer uses pain to counterbalance the potential benefits the enemy could take from achieving his or her strategy. A central theme throughout Schelling's analysis is the use of pain, or the threat thereof, to achieve this end. "To be coercive, violence has to be anticipated. And it has to be avoidable by accommodation."[24] According to him, the advent of nuclear weapons drastically changed the role of destruction in the decision process. While in conventional war,

---

[22] Timothy L. Thomas, "Nation-state Cyber Strategies: Examples from China and Russia," in *Cyberpower and National Security*, ed. Stuart H. Starr, Larry K. Wentz, and Franklin D. Kramer (Washington, D.C.: Potomac Books, 2009), 468.
[23] Schelling, *Arms and Influence*, 2008, 3.
[24] Schelling, *Arms and Influence*, 2008, 2.

military defeat was a preamble to a promise of future hardships, nuclear weapons—and strategic bombing even before made destruction possible regardless of the military fight. Therefore, "War no longer looks like just a contest of strength. War and the brink of war are more a contest of nerve and risk-taking, of pain and endurance."[25]

Robert Pape nuanced this assertion. Questioning the effectiveness of conventional coercion, he categorized its methods following their effects on enemy expected value of resistance. He argued, "the logic of coercion can be described by a simple equation:"[26]

$$R=B * p(B) - C * p(C)$$

Where:	R	=	Expected Value of Resistance
	B	=	Potential value of resistance
	p(B)	=	Probability of attaining benefits by continued resistance
	C	=	Potential cost of resistance
	p(C)	=	Probability of suffering cost

Therefore, he argued, since friendly action can hardly decrease the benefit of resistance (B), coercion can work whether by increasing the cost of resistance (increase C: punishment strategy), or increasing the probability of suffering the cost (increasing p(C): risk strategy), or reducing the probability of gain (reducing p(B): denial strategy).[27]

Pape offered several conclusions. First, "successful coercion based on punishment normally requires the conjunction of three conditions:

---

[25] Schelling, *Arms and Influence*, 2008, 33.
[26] Pape, *Bombing to Win*, 16.
[27] Pape, *Bombing to Win*, 16–38.

low interest by the target; balance of interests favoring the coercer; and balance of capabilities favoring the coercer."[28] On the opposite, he argued, in more serious disputes, punishment usually fails because the balance of interests (including the cost of defeat) in the long term overwhelms the costs.[29] Indeed, the cost of submission includes the political object of war (in the long term), but also the political cost of defeat. In addition, the cost of victory (the punishment) is temporary while the benefits of victory apply on the long term.

Therefore, he came to the conclusion that compellence best worked not through punishment but by denial, through the destruction of enemy military capacity to achieve his objective.[30] This assessment has great merit in clarifying the logic of coercion. Nevertheless, the formula deserves critique. Indeed, for a given outcome, the probability of cost and that of benefits are equal—it is the probability of the strategy to be successful. The strategy value of resistance will be $R = (B - C) \times p(R)$.

Consequently, the concept of risk strategy itself (strategies aiming at raising the probability of cost) is irrelevant. The probability of benefits and cost being associated (since, as Schelling emphasized, an important factor of coercion is the automaticity of retaliation), the only two strategies possible are punishment (raising B) or denial (decreasing enemy chances of success).

---

[28] Pape, *Bombing to Win*, 21.
[29] Pape, *Bombing to Win*, 19–21.
[30] Pape, *Bombing to Win*, 10.

In addition, studying the causes of war, Bruce Bueno de Mesquita came to a similar, although much more developed, formula for expected benefits of conflict.[31] Importantly, he integrated both the immediate utility (expected gain) and the possible shifts of strategy and perspective during the conflict.

Finally, the strategist does not merely examine one strategy, but instead a range of strategic options with a range of possible outcomes, and globalizes the risk of the many possible outcomes. Coercion applies to all of these potential strategic branches, making some more attractive than others.

Conditions for Successful Coercion

Consequently, the success of a coercive strategy depends on several conditions. First, the political end state must grant the enemy concessions—the balance of enemy interests must shift towards the friendly preferred solution both in short and in long term. In addition, the coercer's political and military credibility determine the ability to convince the coerced entity.

First, for coercion to operate there must be a common ground for negotiation.[32] Indeed, when one side seeks the annihilation of the other—whether it is its political existence, its ideology, or its existence as a free

---

[31] Bruce Bueno de Mesquita, *The War Trap* (New Haven, CT: Yale University Press, 1981), 47.
[32] Schelling, *Arms and Influence*, 2008, 1.

state—it can be expected to pursue the fight until the end. In the case of a belligerent seeking to annihilate an entity (usually a regime in that case), coercion cannot operate against the regime itself. It must offer the enemy nation another political structure. Coercion, in that case, does not apply to the regime itself but to smaller entities: political parties or even individuals.

Consequently, the subject of coercion must absolutely and clearly be defined. Is coercion aimed at influencing a regime, or a political element of the regime, or the individuals supporting the regime? This question is paramount because it conditions the methods and operational focus. Fostering regime change may be coercion at the individual level, but it is not at the state level. To make negotiation the best option to the enemy, several levels of coercion may be levered simultaneously, but each exertion of violence must identify accurately what the target audience is and what effects are expected. Thus, examining the elements that led Slobodan Milosevic to yield during the Kosovo war, political scientist and airpower specialist Benjamin Lambeth identified actions at the diplomatic level, threats against Milosevic as an individual (the prospect of trial), but also the possibility of bankrupting Milosevic's domestic supporters.[33] Similarly, Schmitt and Shanker argued that the US antiterrorist campaign against Al Qaeda was in

---

[33] Benjamin S Lambeth, *The Transformation of American Air Power* (Ithaca, NY: Cornell Univ. Press, 2000), 191–192.

essence unconventional deterrence.[34] However, I contend that it cannot possibly be so: how could any strategy persuade an enemy that the desired end state encompasses its own destruction? Instead, the deterrent mechanisms they described operated on the states that supported the organization, and to some extent to the individuals Al Qaeda was willing to engage in terrorist action.

In addition, the domestic political mechanisms that compel the leader must be explicit and take the specific context of politics in times of war. Thus, historian Tami Biddle explained, the interwar debate on population bombing assumed that bombing would terrorize the population and force the leader to surrender.[35] This assumption severely disregarded politics in Nazi Germany, and the polarization and patriotism that arise in time of war.[36]

Finally, coercion must be credible. It must therefore show two characteristics: a material ability to inflict damage that will be superior to the enemy benefit of resistance, and a political determination that leaves no doubt on the automaticity of retaliation. First, the coercer must possess a clear military advantage allowing the exertion of violence while

---

[34] Eric Schmitt, *Counterstrike: The Untold Story of America's Secret Campaign Against Al Qaeda*, 1st ed (New York: Times Books, 2011), 5; 50–56.
[35] Tami Davis Biddle, *Rhetoric and Reality in Air Warfare: The Evolution of British and American Ideas About Strategic Bombing, 1914-1945* (Princeton, NJ: Princeton University Press, 2002), 69–76.
[36] Biddle, *Rhetoric and Reality in Air Warfare*, 78.

denying the same to the coerced.[37] One of the purposes of a conventional conflict is precisely to create this asymmetry that will allow bargaining.

In addition, the potential for damage the coercer holds in reserve must counterbalance enemy perspective benefits of resistance in the long term. Because enemy cost-benefit analysis not only considers immediate hardship but also long-term goals, coercive strategy must address both. As Clausewitz wisely noted, "If the enemy is to be coerced you must put him in a situation that is even more unpleasant than the sacrifice you call on him to make. The hardships of that situation must not of course be merely transient—at least not in appearance."[38] Immediate pain may have short-term effect on enemy strategy, but coercion weighing on long-term enemy interests must involve threatening other interests in a similarly long term. If the coercer wants to influence enemy objectives, he or she must absolutely balance them with the threat of definitive effects.

Airpower historian Mark Clodfelter compared two bombing campaigns in Vietnam and deduced a framework linking political control and effectiveness of strategic bombing.[39] In substance, he showed that Operation Rolling Thunder failed because of an imbalance between positive and negative political aims. President Lyndon Johnson expected ambitious political effects (an independent, stable South Vietnam) but

---

[37] Pape, *Bombing to Win*, 21; Carl von Clausewitz, *On War* (Princeton, N.J.: Princeton University Press, 1984), 77.
[38] Clausewitz, *On War*, 77.
[39] Mark Clodfelter, *The Limits of Air Power: The American Bombing of North Vietnam* (Lincoln, NE: University of Nebraska Press, 2006), xv.

imposed significant negative aims (restrictions to the use of force).[40] On the contrary, Operation Linebacker II aimed merely at bringing North Vietnam to the negotiation table and did not threaten its longer term purpose of reunification. In other words, Nixon used short-term infliction of pain to foster short-term behavior.[41] This example suggests that besides the extent of destruction, the effectiveness of the coercive effects is linked to the durability of the political stake of coercion.

Second, political credibility is equally important. Political scientist Dag Henriksen argued that "the key ingredient in coercive diplomacy is credibility. Since the very nature of coercive diplomacy is the *threat* of force—or the *limited* use of force—it implies a limited use of resources to achieve an objective."[42] In recent conflicts, Western alliances have balanced their lack of political resolve and their political constraints with a tremendous force asymmetry. In consequence, coerced leaders have constantly designed their own escaping strategies to make Western countries reach their political limits.[43] In the coerced mind, the probability of success does not stem from military physical ability to

---

[40] Clodfelter, *The Limits of Air Power*, 203–205.
[41] Clodfelter, *The Limits of Air Power*, 206.
[42] Dag Henriksen, *Nato's Gamble: Combining Diplomacy and Airpower in the Kosovo Crisis, 1998-1999* (Annapolis, MD: Naval Institute Press, 2007), 194.
[43] For instance, Milosevic initially resisted to Allied pressure because he genuinely believed that the retaliation campaign would not last more than a week due to dissention between the Allies (Henriksen, *Nato's Gamble,* 150) Similarly, a probable reason why Saddam Hussein did not yield during the strategic bombing campaign is an incorrect assessment of US will to engage ground troops in a major conventional fight. Consequently, the air campaign could not effectively coerce the regime since it was deemed a temporary evil. Williamson Murray, "Operation Iraqi Freedom, 2003," in *A History of Air Warfare* (Dulles, VA: Potomac Books, 2010), 283.

make victory uncertain but in enemy political constraints, both domestically and internationally. Thus, insurgents have recurrently tried to leverage public opinions to impose political limits to the counterinsurgent's use of force. For instance, the Algerian National Liberation Front—the FLN organized a series of strikes beginning in January 28, 1957. According to Horne, "the principle of the strike followed as a direct consequence of the priority of externalizing the country. It was to coincide with the opening of the UN session."[44]

Coercion, therefore, must closely adapt to enemy strategy to counter any tentative evasive strategy. It is an exercise of persuasion.

[44] Alistair Horne, *A Savage War of Peace: Algeria, 1954-1962* (New York: New York Review Books, 2006), 190.

Chapter 3

Timeless Strategy

As the previous chapter emphasized, the political process inspires much of strategy, from the selection of objectives to the limitations and potential use of force. Exemplified by coercive diplomacy, political purposes appeal to military strategy to twist an enemy's perspectives on the potential costs and benefits of the conflict. The purpose of military strategy, therefore, is to highlight enemy perceptions of the chances of defeat and loss. To achieve this end usually requires suppressing or avoiding enemy military forces. Much of military strategy, therefore, deals with overcoming enemy forces (through annihilation or bypass, for instance).

Two distinct strategic traditions prevail. Eastern strategy, exemplified by Sun Tzu, is in essence subjective. Dwelling on the tremendous costs of war for a state, it considers that limiting force application to the strict minimum is a critical condition for the state not to experience later weakening. Accordingly, a wise use of information aims at altering an enemy's perception and making him or her act unwisely. The acme of strategy is achieving strategic objectives without a

fight. This tradition privileges fostering enemy strategic choices that maximize friendly advantage.[1]

By contrast, Western strategic tradition, epitomized by Carl von Clausewitz's writings, advocates a much more rational, objective approach. For instance, Clausewitz's theory of war acknowledges some subjective factors, but they intervene merely to mitigate the concept of war he manipulates.[2]

Unfortunately, neither of these approaches suffice to apply in cyber-conflict. The human dimension of Eastern approaches, although useful at the tactical level, does not provide any indication on the potential unfolding of conflict in cyberspace. It is a tremendous guide for social engineering but has no explanatory power over the technical dimension of cyberspace. Similarly, the Western strategic wisdom seems unable to transpose the mechanics of war into cyberspace. For instance, the connection between offense and defense, critical to strategy, is not evident in cyberspace.[3] In addition, the objects of Clausewitzian strategy—such as military forces, geography, weather, terrain—fail to transpose simply into cyberspace. Consequently, the wisdom of millennia of strategic theory seems to reach its limits in the virtual world.

---

[1] Samuel B. Griffith, "Preface," in *The Illustrated Art of War*, trans. Samuel B. Griffith (New York: Oxford University Press, 2005), 11–12.
[2] Clausewitz, *On War*,.
[3] In strategy, a possible defensive option is to attack enemy offensive forces, thus transforming offensive might into defensive capability. This is seldom doable in cyberspace. Indeed, attacking enemy cyber-troops does not significantly reduce their offensive capacities.

Yet, some writers have resolutely tried to apply strategic wisdom to the new environment. David Lonsdale investigated the tenets of information war and stated, "It was Clausewitz himself who acknowledged that each age had its own particular character of war, but that there also existed certain universal elements that should be considered. Warfare in the information age exhibits its own characteristics, and even presents significant changes. Yet, the essential nature of warfare, as exemplified in Clausewitz's climate and trinity, remains unchanged."[4]

To adopt a similar approach in cyberspace, it is necessary to bring strategy to a level of abstraction that reflects both Clausewitzian and Sun Tzuian teachings while highlighting notions of strategy that may apply in cyberspace. That is the purpose of this chapter.

Built as a standalone military theory, this chapter describes strategy as "the dialectic of two wills using force to resolve a conflict."[5] Focusing on the essence of military interaction, I conclude that the ancestral discipline of war, at its essence, aims to solve the contradiction existing between the need of planning to achieve the assigned goals, and the adaptation made necessary by enemy strategy. Accordingly, I develop a model that accounts for the intertwining of two strategies and provides

---

[4] David J Lonsdale, *The Nature of War in the Information Age: Clausewitzian Future* (Portland, OR: Frank Cass, 2004), 216.
[5] André Beaufre, *Introduction à La Stratégie* (Paris: Pluriel, 2012), 51. General Beaufre, acknowledging the strategic challenges brought by nuclear weapons, advocates the existence of timeless strategic principles he describes with an analogy to fencing moves.

methodological tools for the strategist to mitigate this contradiction. A way to conceptualize the dynamic nature of war is to study the *time* factor in strategy, how forces evolve over time. This model gets strong inspiration from Clausewitz's description of the ends and means of strategy and of the environment of war. Nevertheless, by introducing information asymmetry as a factor of war and time as a supplementary dimension of strategy, it also account for Sun Tzu's lessons.

International relations theories, military theories and operational domain theories have tried to provide, at different levels, a conceptual framework for leaders to grasp the essential elements of a situation and design the best-fitted strategy. Understanding how this body of theories serves the purpose of the strategist, and how these theories complement (or contradict) each other will be critical to the determination of the questions a cyber-theory will have to answer.

The first requirement of a theorizing process requires identifying the facet of the phenomenon the theory will aim at explaining. A paramount challenge of strategy is to plan for conflict while adapting to the uncertainty of war and particularly that of enemy strategy. A sound military theory must then account for the political nature of war while acknowledging the multilayered organization of states, and therefore of strategy. It must also offer a useable framework explaining the intertwining of confronting strategies.

Accordingly, I examine a model linking objectives, drawn from the political object of war, means and the operational environment. Finally I show that the dynamics of military forces adapting to their environment best accounts for the potential intertwining of strategies. In addition, I explain how planning can mitigate uncertainty, thanks to a thorough understanding of force dynamics.

Ordering Chaos: Theories and Strategy

Only a global approach to strategy can connect the diverse stakes at play in modern conflicts. To achieve this goal, leaders need a conceptual framework to grasp the tenets of a complex situation, plan, and decide. Military theory offers conceptual elements that strategy articulates to design an operational plan, predict its potential outcomes, and assess its effectiveness. The need for a global understanding of conflict requires therefore a global military theory that accounts for the global stakes and which can be broken down into domain theories, when appropriate.

Modern conflicts spread across a broad range of disciplines and involve many state and non-state organizations. They are immensely complex phenomena, involving political stakes both internationally and domestically, soliciting and straining economies, or creating deep and

enduring social disturbances.[6] In wars of attrition like WWI, the strength of the economies, the industrial productive capacities, or the political constraints within both alliances are critical stakes.[7] In Vietnam, domestic and international politics and opinions largely shaped the course and fate of the conflict. In addition, in a massively interconnected world, armed force can no longer disregard these preconditions for success. Military strategies, therefore, must understand and embrace economic, informational, political and societal stakes.

The problem that arises for the strategist, then, is one of prioritization. The tremendous mass of information and parameters that characterizes a conflict, the considerable complexity of the processes involved, and the wide range of possible options require methodological and cognitive tools to grasp the tenets of a situation and elaborate a plan for action. Theories address this complexity issue by isolating a few parameters deemed critical and explaining the mechanisms that underpin the studied phenomena.

In essence, according to strategist Joseph Wylie, traditional theories educate leaders and prepare them to cope with complex situations.[8] Nevertheless, this approach, depending widely on the commander's military genius, becomes increasingly insufficient as the

---

[6] See Stathis N. Kalyvas, *The Logic of Violence in Civil War*, Cambridge Studies in Comparative Politics (New York: Cambridge University Press, 2006), 10, for an extensive account of the social and political disturbance of domestic violence.
[7] Tooze, *The Wages of Destruction*.
[8] J. C. Wylie, *Military Strategy: a General Theory of Power Control* (Annapolis, MD: Naval Institute Press, 1989), 16.

different components of war intertwine. Moreover, the lack of explaining theories fosters cognitive biases penalizing strategies. As international politics professor Yuen Foong Khong pointed out, the use of analogies is a common, if flawed, decisional tool.[9] No two situations are identical and this way of predicting the outcomes of decisions is largely ineffective. Consequently, prominent international relations scholar Kenneth Waltz concluded, "The infinite materials of any realm can be organized in endless different ways. A theory indicates that some factors are more important than others and specifies relations among them."[10]

In essence, theories rationally connect this mass of information and sort the essential from the ancillary. However, they have an instrumental value besides their explanatory power. A consequence of this descriptive value, theories predict the effects of action and are indispensable for planning.[11]

The body of theories available to the military strategist is fragmented along the lines of the social organization of labor. Indeed, modern states' administrations are highly specialized. Thus, in a conflict, the political leadership is responsible for the global strategy of the state, while separate services of agencies manipulate the state's instruments of power. While the writings of Sun Tzu, for instance, have a very holistic

---

[9] Yuen Foong Khong, *Analogies at War: Korea, Munich, Dien Bien Phu, and the Vietnam Decisions of 1965* (Princeton, NJ: Princeton University Press, 1992), 255.
[10] Kenneth Neal Waltz, *Theory of International Politics* (Long Grove, IL: Waveland Press, 1979), 8.
[11] Harold R. Winton, "An Imperfect Jewel: Military Theory and the Military Profession." *Journal of Strategic Studies 34* (December 2011), 2–3.

approach of war, strategic thinkers seem to have followed this trend for specialization, quickly focusing on military strategy, and even domain strategy and subsequent theory.[12] Consequently, international relations theories provide a framework for understanding the behavior of states, thereby allowing for anticipation of the effects of a policy. Similarly, military theories, among other functions, emphasize the important factors at war.

Nevertheless, this artificial division of theory and labor induces severe shortcomings. Indeed, the *nature* of the instruments of power (diplomatic, economic, military and informational) is distinct from their *effects*.[13] Indeed, the actions of each instrument of power affect the whole range of state strategy. Thus, for instance, a blockading army expects to produce economic effects. Fighting an insurrection by winning "the hearts and the minds of the population" is clearly an informational strategy.[14] Finally, strategies of coercion are expected to produce diplomatic, more than military, effects.

The same reasoning holds true for domain strategies. The military services have appeared sequentially and consolidated their organizational

---

[12] It seems useful here to make the distinction between strategy and theory. Strategy is the practical planning and management of a conflict. Theory offers methodological or cognitive frameworks to deal with these highly complex problems. Wylie, *Military Strategy*, 1989, 31; Kenneth Neal Waltz, *Theory of International Politics* (Long Grove, IL: Waveland Press, 1979), 5–6.

[13] This common repartition of instruments of statecraft is particularly Ill described by David A. Baldwin, *Economic Statecraft* (Princeton, NJ: Princeton University Press, 1985), 13.

[14] See, for instance, David Galula, *Pacification in Algeria, 1956-1958* (Santa Monica, CA: RAND Corporation, 2006), xix.

cultures.[15] A part of this culture is of strategic nature. Thus, the military services have fostered the emergence of domain strategies, with a background of inter-service rivalry.[16] However, with the increase in range of weaponry, these artificial boundaries tend to blur and create redundancies within the services.

Furthermore, domain theories potentially have several negative effects on the craft of strategy. First, they tend to underemphasize the final purpose of war, the political object. Indeed, by their very nature, they focus the strategic attention to the subsidiary (although important) purpose of control of a medium. More, they foster rather stereotyped strategy, where the control of the medium precedes attacks of political objectives.

Second, domain strategies downplay the coordination with other components of the state action. Thus, Giulio Douhet advocated reducing the contribution of ground and sea components to self-defense, while the battle in the air would actually decide the fate of conflicts.[17]

Domain strategies are not always irrelevant, however. Discussing the relevance of operational domain strategies, military strategy theorist

---

[15] For a rich discussion on American military services culture, see Carl H. Builder, *The Masks of War: American Military Styles in Strategy and Analysis* (Baltimore, MD: Johns Hopkins University Press, 1989).
[16] Interservice rivalry is especially significant in early domain theorists' works. For Airpower, see Giulio Douhet, *The Command of the Air* (Tuscaloosa, AL.: University of Alabama Press, 2009); William Mitchell, *Winged Defense the Development and Possibilities of Modern Air Power--Economic and Military* (Tuscaloosa, AL: University of Alabama Press, 2009). For the advocacy for an independent thought on naval strategy, see Mahan, *Mahan on Naval Strategy*.
[17] Douhet, *The Command of the Air*, 1998, 213.

Everett Dolman wrote, “Within the overall military strategy, there is room for a set of subordinate strategies to emerge.”[18] Operational strategies make sense when the control of a medium brings decisive advantages in pursuance of the political end. Nevertheless, one must keep in mind that such control has no more value than the opportunities it offers to the overarching strategy. As a subset of any general strategy, operational strategy must be considered in the grander context of general strategy, that seeking nothing but the achievement of political goals.[19]

Therefore, it is my purpose to draw the main lines of a general theory of war. Rear admiral Joseph Wylie advocated for such an endeavor, but he developed a theory based on medium control that resulted in domain strategies.[20] Instead, I will adopt an approach focused on the political ends of strategy that does not presuppose the preeminence of medium control. Aiming at completeness though, it should be able to explain the tenets of domain control when it is required.

To be useful, a military theory must account for the most important characteristics of war. Then it shall offer a model, reducing the strategic situation to a few parameters that allow analysis while offering

---

[18] Everett C Dolman, *Pure Strategy: Power and Principle in the Space and Information Age* (New York: Frank Cass, 2005), 27.
[19] In his exetensive analysis on strategy, Herve Coutau-Begarie warned, the danger of an integral approach to strategy lies in the extreme complexity of the whole of state approach. Hervé Coutau-Bégarie, *Traité de Stratégie*, 5e éd. rev. et augm, Bibliothèque Stratégique (Paris: Institute de Stratégie Comparée: Economica, 2006), 466.
[20] Joseph C. Wylie, *Military Strategy: A General Theory of Power Control*, Classics of Sea Power (Annapolis, MD: Naval Institute Press, 1989), chap. 8.

a realistic account of war. Finally, it deduces logical outcomes from this model.

I will adopt an approach based on a rational actor model.[21] According to this model, state behavior is considered as the fact that of a unitary entity, showing unitary will, and acting rationally according to its interests.[22] Rationality simply means the state wills elect among known options those that provide it the greatest benefit.

This approximation disregards several factors. First, armies have an extremely strong identity and organizational inertia. According to operational analyst Carl Builder, "The roots of modern American military strategies lie buried in the country's most powerful institutions: the Army, the Navy and the Air Force."[23] According to Allison and Zelikow, their organizational inertia and bargaining power account for much of the strategies implemented.[24]

Second, the division of labor in effect in most advanced countries favor "segment strategies."[25] Most services and agencies tend to develop a

---

[21] Graham T Allison and Philip Zelikow, *Essence of Decision: Explaining the Cuban Missile Crisis* (New York: Longman, 1999), 16–18.In this analysis of the Cuban missile Crisis, the authors describe three models describing state behaviors. The most simplistic one, the rational actor model, disregards the parameters that might make states' behaviors deviate from purely "rational" decisions. The behavior of the state is therefore explained by its aims and calculations (13).
[22] For a more detailed description of this model, see Allison and Zelikow, *Essence of Decision*, 16–19.
[23] Builder, *The Masks of War*, 4.
[24] Allison and Zelikow, *Essence of Decision*, 379–385.
[25] By segment strategy, I refer to the application of the instruments of power (diplomatic, informational, military and economic—DIME) in their respective areas. For instance, in the case of the USA, the segregation between DOD strategy and DHS strategy, even despite cooperation, create potential inefficiencies.

strategy for their segment—military services implement military strategies to overcome the enemy—regardless of the other instruments of power and subsequent strategy.

Having made the stakes of a theory of conflict clear, a first requirement emerges. A model being a simplification, a schematization of reality, its shape must stem from the elements that have most influence on the conduct and consequences of a conflict. I must therefore characterize the nature of strategy in conflicts.

Characteristics of Strategy

Whatever the level of war considered, war is above all a complex social phenomenon, one that involves men and women and challenges their ability to overcome and outsmart their adversary. The fundamental problem of any strategy of conflict, therefore, is to reconcile the two contradictory challenges that await the practitioner. On the one hand, achieving the political goals of the conflicts, successfully using large assets despite enemy resistance, requires thorough planning and anticipation. On the other hand, the planning process itself must take into account the enemy potential for surprise and leave room for adaptation. The contradictory needs for planning and adaptation characterize best the problem arisen to the strategist.

As political goals alone define the ends of strategy—as conflicts are merely instruments of states' politics—the foremost quality of strategy is

predictability. To be of some utility to political leaders, military strategy has to predict outcomes. "If the essence of strategy is instrumentality, the essence of instrumentality is predictability."[26]

In addition, achieving political goals requires the performance of complex processes that require time and thorough planning and coordination. For instance, a state's strategy in conflict requires coordinating military strategy with diplomatic effort and economic and industrial policies. During WWII, the mobilization of human and industrial resources was critical to the generation of US and British military power and the military strategy encompassed this gradual increase and targeted German industrial capabilities. These efforts, aiming at shaping the balance of military forces between the Axis and the Allies were long reaching, aiming several years from when the respective war plans were decided.[27]

Unfortunately, conflicts arise when states do not forecast the same outcome of the conflict. Wars develop in unexpected ways, through mutual adaptations—Moltke stated, "Plans rarely survive the first encounter with enemy forces."[28] Therefore, the reason strategy transcends the science of military theory and enters into the realm of an

---

[26] Colin Gray, *Strategy for Chaos: Revolutions in Military Affairs and the Evidence of History* (London, UK: Frank Cass, 2002), 98.
[27] Biddle, *Rhetoric and Reality in Air Warfare*, 206; 211.
[28] Helmuth Moltke, *Moltke on the Art of War: Selected Writings*, trans. and ed. Daniel J. Hughes (Novato, CA: Presidio Press, 1995), 45.

art is the need to take into account enemy reaction.[29] Much of the challenge of strategy is therefore to minimize the effects of war's unpredictability.

Indeed, conflicts are not in the realm of predictability, despite the recent efforts in modern armies to make war as deterministic as possible.[30] Thus, Carl von Clausewitz suggested that several factors blurred and jeopardized the deterministic logic of the balance of forces. First, information is partial, subject to interpretation and delusion.[31] Although modern conventional forces have sought to reduce the fog of war through improvement of ISR capabilities, the essentially human nature of war leaves social areas unobserved.[32]

Enemy behavior reinforces this uncertainty. Military genius, as Clausewitz put it, is quite unquantifiable and weighs heavily on the fate of battles despite force ratios. Great strategists have been those able to conciliate long-term goals and short-term adaptation. For instance, the foremost quality of chancellor Otto von Bismarck's grand strategy was his flexible eventual goal and clever ability to adjust his strategy and planning as events unfolded.[33]

---

[29] Clausewitz, *On War*, 149.
[30] Lonsdale, *The Nature of War in the Information Age*, 2004, 4–5.
[31] Clausewitz, *On War,* 84-85. Acknowledging the "imperfect knowledge of the situation", he argued that "each side, using the laws of probability, forms an estimate of its opponent's likely course and acts accordingly."
[32] Lonsdale, *The Nature of War in the Information Age*, 2004, 9.
[33] Marcus Jones, "Strategy as Character: Bismarck and the Prusso-German Question, 1862-1878," in *The Shaping of Grand Strategy: Policy, Diplomacy, and War*, ed. Williamson Murray, Richard Hart Sinnreich, and James Lacey (New York: Cambridge

I will therefore construct a military theory to account for this paramount dimension of war. The choice of adequate variables will delineate the main driving forces at play in strategy.

A Basic Model: Objectives, Actors and Factors

A first step of theorization aims at simplifying, modeling the operational environment according to the theory's intent. Given the scope of this document, which is aimed at practical strategy, a model must highlight the relationships between the means and the political outcomes of strategy. In addition, it must also account for the factors that influence these variables in ways susceptible to altered strategies. Therefore, I will categorize the elements of strategy between objectives, actors, and factors.

University Press, 2011), 108. Jones assessed, "in a world in which outcomes are indeterminate, competent strategy consist (…) a clear understanding of one's principles and priorities and a flexible, creative approach to realizing incremental gains in the short term." Jones, "Strategy as Character: Bismarck and the Prusso-German Question, 1862-1878,"

Objectives: Military objectives must be considered through their contribution to the eventual settlement of the conflict. They are to some extent part of the desired end state. As international politics scholar Fred Iklé pointed out, statesmen should always take into account war termination and envision the forces, actors, and political balances after the war.[34] Military objectives pertain to this end state: shaping the political balances, they encompass much more than overcoming enemy armies.

As Clausewitz emphasized, "To overcome the enemy—or disarm him—must always be the aim of warfare."[35] In this approach, the military objective involves destroying enemy military forces; making him defenseless and unable to exert a threat. In that case, the military objectives are enemy military centers of gravity, "hubs of power and movement."[36]

This strategy may nevertheless prove too costly for limited objectives, and, in some instances, may be irrelevant. Indeed, whether due to the international context, or to domestic restraint, military superiority alone does not convince the enemy of immediate danger. In most UN resolutions, territorial integrity is not at stake, nor is the government.

---

[34] Iklé, *Every War Must End*, 2.
[35] Clausewitz, *On War*, 77.
[36] Clausewitz, *On War*, 596.

In addition, an inferior enemy can also remain harmful even if significantly disarmed, through action in the political realm. Thus, insurgency tactics have recurrently displaced the fight into the informational, and therefore political, arena.[37]

Therefore objectives can address centers of gravity in various realms. For instance, as French historians Pierre and Marie-Catherine Villatoux showed, propaganda has not been used merely against neutral populations during insurrections, but also against modern, organized armies to threaten their cohesion and hamper their effectiveness.[38]

Finally, political objectives encompass positive and negative objectives. Positive objectives are those that have to be taken: land, enemy forces, sea routes, enemy political will. Negative objectives, by contrast, are defensive ones: protecting national lands, states or governments.[39] Self-preservation is usually the minimum objective of any belligerent. Nevertheless there is a hierarchy between positive and negative political goals. Usually, negative goals, especially preservation, are held dearer and therefore have a higher priority.

Conflict theorists are split on the value of objectives in strategy. Some argue that objectives are attributes of tactics, while strategy should

---

[37] The general strike organized by the FLN to export the Algeria war to the international community is a good example of this politicization. See Horne, *A Savage War of Peace*, 190.
[38] Paul Villatoux and Marie-Catherine Villatoux, *La République et Son Armée Face Au Péril Subversif: Guerre et Action Psychologiques En France, 1945-1960* (Les Indes savantes, 2005), pt. 1.
[39] Clausewitz, *On War*, 358.

concern itself with gaining the greatest possible advantage. Thus, Helmuth Von Moltke advocated, "Strategy can direct its endeavors only towards the highest goal attainable with the means at hand."[40] In a similar approach, Everett Dolman emphasized the perpetual and continuous nature of strategy that shall not seek the achievement of objectives but that of a continuous advantage.[41]

This notion of maximization assumes the ability to measure advantages on an unambiguous scale. In Moltke's mind, this meant conquering as much territory as possible, or destroying as much of the enemy forces as was possible with the means at hand. Such a maximization approach may threaten other state objectives such as postwar political balance.

There is little doubt that the desired end state, the object of war, should be constantly adapted to the evolution of the geostrategic situation, and the military objectives should follow accordingly. As Defense specialist Richard Sinnreich noticed, grand strategy is more effective when general principles guide a pragmatic and adaptive approach.[42]

---

[40] Moltke, *Moltke on the Art of War*, 36.
[41] Dolman, *Pure Strategy*, 2005, 5–6.
[42] Richard Hart Sinnreich, "Patterns of Grand Strategy," in *The Shaping of Grand Strategy: Policy, Diplomacy, and War*, ed. Williamson Murray, Richard Hart Sinnreich, and James Lacey (New York: Cambridge University Press, 2011), 256.

Actors: Strategy professor Hervé Coutau-Begarie offered an interesting model to shape theory. Indeed, he distinguished two categories of variables at play in strategy. The actors are "the strategists themselves, but also all those who will intervene, in one way or another, in the strategic process."[43] By contrast, the factors are "the elements on which man has no immediate grasp … They generate constraints or opportunities the actors may take into account to overcome them or take advantage of them."[44] Thus, the actors are the means of strategy, while the factors are the variables that affect their behavior and effectiveness.[45]

Two concurrent approaches regard the means of strategy differently concerning the strategist. One considers strategy as a chess game: war, for them, is the opposition of two wills, a duel.[46] Accordingly, friendly and enemy strategists are therefore outside the means, because they are using these means to achieve their ends. The other trend considers belligerents as complex, adaptive systems that react to their environment, and therefore incorporate the strategy-making process in the forces system.[47] Both offer significant explanatory power, but lead to

---

[43] Hervé Coutau-Bégarie, *Traité de stratégie* (Paris: Institut de stratégie comparée: Économica, 2006), 312.
[44] Coutau-Bégarie, *Traité de stratégie*, 312.
[45] For Clausewitz, physical forces were the means of tactics while engagements were the means of strategy (Clausewitz, *On War*, 1984, 142). However, as baron Antoine-Henry de Jomini explained, the art of strategy involved provides forces in time and place of engagement. It is therefore hardly relevant to consider forces only at the tactical level. Antoine Henri Jomini, *The Art of War* (Mineola, NY: Dover Publications, 2007), 62.
[46] See, for instance, Beaufre, *Introduction à La Stratégie*, 34; Clausewitz, *On War*, 75.
[47] For instance, Frans P. B Osinga, *Science, Strategy and War: the Strategic Theory of John Boyd* (London; New York: Routledge, 2007); David Kilcullen, "Countering Global

very different conclusions. The former approach focuses on the craft of strategy, while the latter advocates efforts on friendly structure and enemy environment to modify the way enemy and friendly systems behave.

The purpose of this theory is to explain how strategists interact. Therefore, I chose the first approach. Strategists, therefore, are not part of the system they are using in pursuance of their objectives. *The actors considered here will be the means made available to the strategist to fulfill state objectives*.

The political ends of a conflict motivate strategy. Strategy being the art of connecting ends and means, the means of strategy must relate directly to the ability to achieve political end. Therefore, I will employ the word *force* for any means that possess the ability to produce forcible political effects—that is, contribute to the political objectives.

The diversity of political leverages and that of the ways to achieve these leverages define that of the means of strategy. The nature of *forces* depends on that of *objectives*. "Forces are the means of war," [48] Clausewitz contended. Here, the only extension I add to his thinking stems from the fact that the range of political objectives has significantly extended, then so has the range of the means of strategy.

Insurgency," ed. Thomas G Mahnken and Joseph A Maiolo, *Journal of Strategic Studies* 28, no. 4 (2005): 597–617.

[48] Clausewitz, *On War*, 75.

Given that the enemy military represent an important strategic objective, the means of strategy encompass the forces that can defeat them or destroy enemy military effectiveness. In addition, coercive action also produces political effects. The possible leverages can also be political, economic, or social. State strategies can leverage them through the whole range of the instruments of power. As such, the military can exert violence on these centers of gravity regardless of their pure military value.

Factors of War: The factors of war are the external conditions that affect forces. Clausewitz identified several of them, selected for their effects on the outcome of the engagement.[49] To exemplify the nature of their effects of environmental factors on forces, I will give a closer look to the influence of geography and information on strategy.

The inclusion of contextual inputs into strategy stems from the fact that forces are not static variables. Interacting with their environment (and with enemy forces) they lose their effectiveness, disappear, or on the contrary gain momentum and regenerate following the conditions they meet.

A critical factor in war is geography. Military theorist baron Antoine-Henry de Jomini studied in great detail how geographic features influenced land warfare. His analysis of lines of communications and

---

[49] Clausewitz, *On War*, 142–143.

their connection to objective points brought him to a geometric approach to strategy. [50] Similarly, Clausewitz provided an extensive analysis of the effects of geography on offensive and defensive strategy in his Books 6 and 7.[51] In essence, geography has two distinct effects. Distances and rough terrains hamper the access of offensive forces to an objective and reduce military effectiveness.

This teaching, particularly important during Napoleonic wars, is still valid today. Even motorized troops are more vulnerable to attacks while moving. In addition, geography can provide distinct defensive or offensive advantages. Thus, high grounds and fortified areas benefit to defense while dense vegetation provides the offense with effect of surprise.

In addition, information influences strategy in two different ways. As strategist Franz Osinga argued, a purpose of strategy is the destruction of mental images, in order to prevent enemy adaptation to actual conditions of war. Thus, information is a prerequisite to operational effectiveness: it conditions the very ability to use force. Sun Tzu wrote extensively on the strategic value of informational superiority. In fact, his teachings describe to a great extent how information superiority can balance physical strength.[52]

---

[50] Jomini, *The Art of War*, 78–83.
[51] Clausewitz, *On War*, 357–573.
[52] Griffith, "Preface," in *The Illustrated Art of War,* 12.

This model describes the elements belligerents must take into account to achieve their objectives. The bulk of strategy requires overcoming enemy attacks or resistance. My model must encompass an additional dimension that accounts for the intertwining of two strategies fighting for contradictory objectives with opposed forces that try to exploit their environment.

Tenets of Strategy

To capture the essentially interactive aspect of strategy, an extra dimension is needed. Indeed, describing the unfolding of competing strategies makes it necessary to consider the effects of factors—and engagements—not in a static way but in a dynamic one.

As I have shown, strategy aims at planning the use of forces in order to achieve objectives despite enemy potential for surprise. Napoleon Bonaparte stated that an important quality of the strategist rests in his ability to consider every possible unfolding of the battle in order to design a plan. Thus, a plan should ambition to consider every possible action of the enemy and mitigate its consequences.

In the field of risk analysis, two options exist to mitigate a risk associated to a given event. First, it is possible to mitigate the undesirable outcomes of the event. Second, it is possible to reduce the

probability of this undesired event to happen. This principle applies as well in strategy.[53]

The first option is rather static and defensive in nature and therefore reactive. Indeed, it relinquishes initiative to the enemy. It involves, for instance, hardening defenses, or setting procedures to cope with disruption. Nevertheless, it simplifies friendly strategy because it allows neglecting taking into account a range of possible enemy actions and focusing on those that have a significant residual impact.

The second option aims at reducing the range of enemy options. This may include either applying the logic of coercion to enemy strategic options, or forcing the enemy to engage its forces in defensive actions. Indeed, friendly actions may influence enemy risk-benefits analysis of potential courses of action. Thus, Sun Tzu essentially described war as an art of deception.[54] The purpose is to convince the enemy that some strategic options will either be ineffective, or too costly, or will probably fail.[55]

Alternately, the enemy can be forced to react to friendly strategy. The principle of initiative dwells on this opportunity: confronted with a

---

[53] Bernard Brodie, *Strategy in the Missile Age* (Santa Monica, CA: RAND Corp., 2007), 181.
[54] Sun Tzu, *The Illustrated Art of War*, trans. Samuel B. Griffith (New York: Oxford University Press, 2005), 96.
[55] Carl von Clausewitz acknowledged the importance of this calculation from the strategic to the tactical level. Thus, he wrote, "The fact that engagements do not always aim at the destruction of the opposing forces, that their objective can often be attained without any fighting at all but merely by an evaluation of the situation, explains why entire campaigns can be conducted with great energy even though actual fighting plays an unimportant part in them. "Clausewitz, *On War*, 96.

threat, the enemy has no other option than to react to friendly actions. Moltke considered it the best explanation why, despite the rational advantage of defense, the offensive had often been successful in the past.[56] Similarly, Clausewitz emphasized the principle of offensive defense because it allowed taking advantage both of the strategic advantage of defense and the operational advantage of initiative.[57]

To take advantage of this strategy, a deep understanding of the effects of factors over time is necessary. Napoleon Bonaparte once stated, "Strategy is the art of making use of time and space. I am less chary of the latter than the former. Space I can recover, time never."[58]

Indeed, a critical determinant of engagements is the local balance of forces.[59] Thus, even with a globally inferior army, Napoleon usually managed to achieve a favorable balance of forces at the moment of the critical engagements. Achieving this balance requires identifying the factors that will provide an advantage over the enemy and engage when these factors create the most favorable balance.[60]

At any given time, whether used or not, the forces of belligerents have an ability to inflict damage, or to absorb enemy forces.[61] Thus,

---

[56] Moltke, *Moltke on the Art of War*, 47–48.
[57] Clausewitz, *On War*, 361.
[58] Osinga, *Science, Strategy and War*, 191.
[59] Clausewitz, *On War*, 282–283.
[60] Basil Henry Liddell Hart, *Strategy* (New York: Meridian, 1991); Clausewitz, *On War*, 194.
[61] Interestingly, game designers have rightly understood this basic component. For instance, Pokemon cards measure the fighting abilities of a figure by an attack value

Clausewitz identified several categories of factors that affected strategy.[62] To be more accurate, it is the effects they have on forces that define their effects on strategy. Now, these effects are usually temporary. Thus, the effect of surprise has a very limited psychological effect and the limits of its strategic effect depend on the position of enemy reserves.

The retention of initiative in strategy, therefore, involves assessing the time the enemy needs to adapt to friendly attacks and synchronize stimuli on the enemy's system faster than he can bear. According to Osinga, this strategy would provoke enemy disaggregation.[63]

Dynamics of Forces

This section provides the reader with some basics on the dynamics of forces. It describes succinctly how two different strategic approaches to force dynamics can produce very different forms of war.

At the state level, strategy concerns itself with the generation and utilization of forces. Its primary aim is to generate forces necessary for victory. Thus, regardless of military strategy, US intrinsic ability to produce large quantities of technologically advanced materiel would

---

and a defense value. It is a very basic model though, where only conflict can alter forces (regardless of environment, psychology, logistics…).

[62] Clausewitz, *On War*, 183.

[63] Osinga, *Science, Strategy and War*, 184–186.

eventually allow the Allied forces to prevail in WWII.[64] Similarly, Mao Zedong's strategy against Japan dwelt on the fact that through propaganda, external support, and capture of enemy materiel, the Chinese would eventually possess the means to challenge and vanquish an initially superior Japan.[65]

Consequently, two basic forms of warfare coexist, characterized by both their strategic objective and their relation with forces. [66] Wars of attrition essentially challenge the participants on their respective ability to generate forces. Therefore these are usually protracted conflicts, lasting for several years.

On the contrary, wars of movement seek the temporary paralysis of the enemy's forces to reach the enemy's vital points for a rapid settlement. These wars are extremely compressed in time. The underlying strategy aims at challenging enemy capacity to adapt to friendly action. The German *Blitzkrieg* is the most famous example of this form of warfare.

---

[64] While German war economy plans Ire calibrated for a short war, the ability of the Allies to engage Germany in a long lasting arms race eventually led to its collapse. Tooze, *The Wages of Destruction*, 667.
[65] Mao Tse-Tung, "On Protracted War," May 1938, http://www.marxists.org/reference/archive/mao/selected-works/volume-2/mswv2_09.htm (accessed 20 May 2013).
[66] Boyd described a third form of war, the psychological one. Nevertheless, following the strategic objective and subsequent pattern (whether the objective is to threaten political centers of gravity (COGs) before the enemy can react or destroy enemy forces to reach their COGs), psychological wars can be sorted in the former two. Osinga, *Science, Strategy and War*, 166.

This categorization transcends the object of war and the nature of belligerents. Thus, revolutionary warfare and *Blitzkrieg* pertain in strategies of movement, while protracted warfare exists both in state on state conflicts (attrition wars) and in insurgencies (protracted insurgencies).[67]

Conclusion

This chapter has gathered pieces of classical strategic wisdom in terms that are intended to be applicable to cyberspace. To offer logical coherence, this knowledge was presented as a standalone theory.[68] Nevertheless, its purpose is really to federate valuable wisdom and make it useful for cyber-strategy.

To account for the link between the assets available to the strategist and the ends he pursued, the model I adopted describes forces as the means to achieve objectives. Therefore, forces have to be defined according to the nature of objectives. Yet, they are not static variables. They depend on a variety of external factors from their operational environment.

---

[67] Both Mao and Lawrence emphasized the eroding purpose of guerrilla warfare. The primary purpose of such strategies is not a specific strategic point. Guerrilla warfare aims at exhausting enemy forces until they can be fought conventionally.
[68] The conclusion of this paper recapitulates the elements of this theory following Harold Winton's criteria of military theory.

Finally, I argued, strategy is hard because it requires planning while enemy strategy requires adaptation. To solve this contradiction, three categories of solution exist. To reduce the *effect* of enemy strategy, friendly forces can shield their centers of gravity and mitigate the operational consequences of enemy attacks. To reduce the *range* of enemy strategic options, friendly strategy can influence enemy cost-benefit analysis in a similar way to the logic of coercion explained in Chapter 2. Finally, keeping the initiative forces the enemy to *react* to friendly stimuli and therefore prevents surprise. To achieve enduring initiative, it is paramount to understand the time needed by enemy forces to adapt, and synchronize friendly action to outpace and disrupt enemy adaptation process.

Chapter 4

A Strategy of Bits and Peaces

The past two parts have highlighted several aspects of conflicts. Their instrumentality in international politics stems from the bargaining leverage a favorable military situation offers. The underpinning logic of coercion drives the enemy to reconsider cost-benefit calculations. In other words, an effective coercive action aims at either depriving the enemy of the prospect of gain, or at acquiring the certitude of painful development should the conflict endure.

To achieve this end, military strategy employs forces to achieve strategic objectives. A paramount aspect of strategy lies in the understanding of the external factors that modify friendly and enemy forces. The dynamics of these forces, the pace and extent of evolution of military forces, constitutes a critical aspect of the study of strategy.

Projecting these concepts into cyberspace is the purpose of this chapter. To do so, it was first necessary to characterize the tactical tenets of conflicts in cyberspace. The (defensive and offensive) exploitation of vulnerabilities appears as the critical aspect of cyber-attacks, and therefore cyber defense. Therefore, cyber-forces have to be defined as the means that manipulate vulnerabilities in furtherance of cyber-objectives.

The principal factor affecting these forces is cyber-geography. This denomination designates the physical implantation of components of cyberspace, but also other layers of great strategic importance. Thus, the functional structure of cyberspace is another strategically significant aspect of cyber-geography as well as the manufacturing origins of the critical components of cyberspace.

Implementation of the model offered in Chapter 3 allows the drawing of some conclusions about cyber-strategy. According to its lessons, two solutions may reduce the uncertainty linked to enemy initiative. The first one is to force the enemy to react constantly. The element of initiative is key to maximize the strategic effects of cyber-offensive. The second option is to minimize the impacts of enemy action. This mode of action underpins cyber-security. Nevertheless, the perspectives of active defense in cyberspace deserve scrutiny. Although nonexistent today, active defensive strategies could become more relevant in a context of prolonged cyber-war.

Consequently, the development of cyberpower should dwell on these principles. Shaping cyber-geography both domestically and internationally would provide a significant advantage in the advent of conflict. In addition, the development of human capital in cyberspace should include both increasing research capacities and operational structures.

Instantiating theory

Cyber-Tactics: A first step towards cyber-strategy requires that I understand the tenets of cyber-tactics. Cyber-attacks and therefore cyber-defense exploit or protect *vulnerabilities* to produce cyber-effects. Vulnerabilities are potential weaknesses, inherent to technological and human systems. Their exploitation or correction is the major tactical stake in cyberspace.

According to the EBIOS risk management method (Etude des Besoins et Identification des Objectifs de Sécurité or Study of requirements and identification of security objectives), a vulnerability is "the characteristic of an asset that may constitute a weakness or a breach in the security of the system."[1] This definition does not only relate to the technical weaknesses (e.g., a software "bug"). It also includes all the constituting elements of a system: physical components, energy, infrastructure, procedures and personnel.[2] Each of them has potential vulnerabilities that an attacker can identify and exploit.

Infrastructures have vulnerabilities. Indeed, buildings can offer a limited resistance to fire or bombing, the roofs or floors can be subject to penetration by trained teams. Computing devices can also have embedded vulnerabilities. They can be malfunctions due to a poor design

---

[1] ANSSI/ACE/BAC, "EBIOS - Risk Management Method," January 2010, 94.
[2] For an exhaustive categorization of vulnerabilities, see ANSSI/ACE/BAC, "EBIOS - Risk Management Method," 54–59.

or quality control, but they can also have undocumented functions that an attacker can use to bypass software security. Probably the most famous category of vulnerabilities, software weaknesses plague most commercial software. As for device vulnerabilities, they can be due to designer negligence or undocumented functionalities that have been created on purpose. Finally, humans and organizations also have vulnerabilities.[3] Although human weaknesses can hardly be patched, organizations create a set of policies and procedures to mitigate the risks due to human factors.[4] These procedures, too, can have weaknesses, neglect possible scenarios, or include inconsistencies.

Although all these vulnerabilities do have applications and are considered by both attackers and defenders, technical vulnerabilities (that is, those embedded in hardware and software) are of specific interest because they are constitutive of cyberspace. They determine the possible range of the attack, its criticality, and the ability of defenders to protect against a category of attacks. They constitute the specificity of fighting *in* cyberspace.

At first look, one could assume that vulnerabilities exist in limited numbers and could be eradicated if systems were designed correctly. Several factors suggest that it is not so. First, the increasing complexity of software and hardware make it accordingly more difficult to control

---

[3] Christopher Hadnagy, *Social Engineering: The Art of Human Hacking* (Indianapolis, IN: Wiley Publishing Inc., 2010), 4.
[4] Hadnagy, *Social Engineering*, chap. 9.

and envision all the possible interactions and outcomes.[5] Some formal methods allow proving portions of code and ensuring that its behavior complies with specifications. Nevertheless, these methods need unambiguous specification of all possible cases and, in addition are usually not economically viable.[6]

Second, for a mix of economic and operational reasons, many cyber-assets cannot afford an extensive security review. While the operational functions are usually abundantly tested, security tests are sometimes more constrained in part because they are not readily observable.

Cyber-attacks, therefore, take advantage of a succession of vulnerabilities to create a robust scenario that is intended to take control of, disrupt, or destroy the target system. The craft of cyber-attack, and the techniques to defend against these, are wholly centered on the discovery, exploitation, detection, or correction of vulnerabilities. They constitute the tactical level of cyber-conflict. To come to cyber-strategy, it is therefore necessary to articulate how the use of cyber-battles can contribute to the achievement of political and military objectives.[7]

---

[5] Libicki, "Sub Rosa Cyber-War," 5.
[6] Daniel M. Berry, "Formal Methods: The Very Idea: Some Thoughts About Why They Work When They Work," *Science of Computer Programming* 42, no. 1 (2002), 11–27.
[7] To paraphrase Carl von Clausewitz, "strategy is the use of the engagement for the object of war." Clausewitz, *On War*, 128.

Cyber-objectives: Cyber-objectives are entities, accessible through cyberspace, whose leverage produces strategic effects. Indirect (military) objectives enable further action towards a political center of gravity, while direct (strategic) objectives influence the strategic calculations of the enemy.

The first category of objectives is similar to current military practices in physical domains. In a similar fashion to the physical exertion of violence, cyber-attacks can destroy or disrupt systems related to enemy defensive or offensive forces, whether directly or indirectly. Thus, the disabling of enemy grated air defense system (IADS) provides a direct military advantage that can be exploited in the broader context of the campaign. The disruption of an oil distribution system or of electric distribution indirectly harms enemy effectiveness, thereby providing a military advantage.[8]

Using cyberspace to attack military objectives offers specificities a military commander can take advantage of. First, cyber-attacks can be more furtive than kinetic actions. The operational effect can therefore be maximized since the enemy does not react as long as he does not perceive the disruption. In addition, side effects of attacks (casualties or disruption of civilian activities) can be felt as more trivial due to the

[8] In "Ten Propositions Regarding Cyberspace Operations," *Joint Forces Quarterly*, quarter 2011, 11, Major General Brett Williams laments the lack of emphasis on the operational level of cyber-war and offers several suggestions for its development.

virtual nature of cyber-attacks (the acceptance threshold seems to be higher for cyber-attacks).

The second category, on the other hand, that of strategic objectives, expects very different effects from destruction or disruption. In a coercive logic, destruction or disruption is not intended to impair enemy forces, or even enemy population. Instead, as I have suggested in Chapter 2, it forces the enemy to a new risk-benefits calculation. Whether raising the expected cost of opposing friendly objectives or denying enemy prospect of victory, strategic action influences enemy expected outcomes of his strategy. Coercion is a promise, it provides clues on future developments of the conflict should disagreement persist.

While operational cyber-objectives can be expected to be confined to national security networks, strategic cyber-objectives can rest on the Internet or within civil agencies and civil operators of enemy state.[9]

These two broad categories of cyber-objectives can concretely take several forms.[10] When the objective is a function that must be disrupted, the objective can be a whole system. Thus, for instance, disrupting the enemy IADS capability involves destroying key elements of the underlying

---

[9] For an extensive description of the potential use of strategic cyber-attacks, see Richard A. Clarke and Robert Knake, *Cyber War: The Next Threat to National Security and What to Do About It* (New York: HarperCollins, 2010).

[10] I have purposefully excluded the use of cyberspace for influence. This kind of operation is not cyber-conflict, more information warfare in cyberspace. According to the definition offered in Chapter 1, the semantic layer of cyberspace has been evicted from the scope of this study.

system (those elements that are in cyberspace). Alternately, a cyber-objective can also merely be critical data.[11]

To achieve these cyber-objectives, cyber-strategy needs to define its means, the forces made available to the strategist.

Cyber-Forces: Since the exploitation of vulnerabilities is the intent of the tactical level of cyber-conflict, forces are the means that manipulate them to achieve strategic objectives. Defensive and offensive cyber-forces are divided into research forces, that generate or fix vulnerabilities, and operational forces, that turn technical vulnerabilities into operational effects.

An unusual characteristic of cyber-struggle is that a critical stake for the offender lies in the defender's hand. Cyber-weapons are not assets; they are knowledge on enemy vulnerabilities. Therefore the offensive means of cyber-strategy are the friendly assets that generate and exploit this knowledge. In a similar fashion, the defensive means are those that detect attacks, mitigate their operational effects and correct the vulnerabilities exploited.

First, these capabilities (both offensive and defensive), depend on *research forces*. These forces are constituted of engineers, researchers or antivirus labs that either analyze software and hardware to find potential vulnerabilities and the ways to exploit them, or that analyze emerging

---

[11] Joel Brenner emphasized the understated value of critical data in Brenner, *America the Vulnerable*, 25–26.

attacks to understand their technical origins and find ways to correct the underlying vulnerabilities.[12]

Second, *operational forces* are also necessary to link technical knowledge with operational effects. Indeed, the process of discovering or correcting vulnerabilities has no effect *per se*. To build offensive capabilities, they must be integrated with other types of knowledge (intelligence on targeted systems, organizational structure, culture and procedures of the enemy). Similarly, defensive operational forces are civilian and military operators that control the security of the system, try to detect clues of stealthy takeover or attempts to test the system's vulnerabilities. When an attack occurs, they try to stop it and mitigate its operational effects.[13]

---

[12] Stuart H. Starr, "Toward a Preliminary Theory of Cyberpower," in *Cyberpower and National Security*, ed. Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz (Washington, D.C.: Potomac Books, 2009), 49. The author categorized the intellectual capital required for cyberpower along three lines. The personnel detaining technical expertise (which he identified as cyberspace experts) correspond roughly to the "research forces" described here. The cyberpower experts are the operational forces described later. He added a third category of cyber-strategy experts, which I identified as the cyber-strategists who, according to the model offered in Chapter 3, are outside the scope of this discussion.

[13] Edward Amoroso, *Cyber-attacks: Protecting National Infrastructure* (Burlington, MA: Butterworth-Heinemann, 2010), chap. 10–11.

Cyber-geography: To the strategist, the aspects of cyber-geography that matter differ from that a civilian geographer would focus on. While cyber-geographers concern themselves with the flows of data or the social aspects of cyber-geography, the cyber-strategist examines the aspects of cyber-geography that affect cyber-forces and cyber-objectives. Three parameters are particularly significant from a cyber-standpoint: physical control, manufacturing origins and functional structure.

Geographers study not only the shape and structure of Earth; they also study its effects on human activities and interactions. Meanwhile, the strategist views geography mainly across the parameters that influence the application of force or the access to strategic objectives. In a similar fashion, cyber-geography at large has studied the structure of cyberspace mostly through its social effects. Therefore, cyber-strategists must examine the elements of cyberspace topography that influences either the effectiveness of cyber-forces or their ability to reach cyber-objectives.

The relation of geography to cyberspace is mixed. On the one hand, some geographers argue that "the whole notion of geographic space is destroyed and geographic location is not relevant at any scale."[14] According to this view, "Cyberspace has geographic implications but it is transforming space-time relations and creating new social spaces that

---

[14] Guoray Cai, Stephen Hirtle and James Williams, "Mapping the Geography of Cyberspace Using Telecommunications Infrastructure Information," *TeleGeo* (1999), 147.

lack the formal qualities of geographic space."[15] This view argues therefore for a functional, rather than physical, representation of cyberspace.

Functional architecture of cyberspace is indeed critical to the strategist, since it represents how the different constituting parts of that medium depend on each other and provide services to its users. Accordingly, some elements of cyberspace have critical importance. Thus, the servers that handle users' and machines' identities are central to a system's health. Similarly, at a lower level, nodal routers play the paramount role of coordinating the traffic. On the defensive side, some specific elements like firewalls and other security infrastructure contribute to a system's security. Attackers have to go through several layers of protection to reach their objectives. Enemy cyber-geography defines friendly exterior lines.

Nevertheless, Cai *et al* argued, geography has an effect on all the layers of cyberspace.[16] For instance, they showed that the notion of distance could be associated to the time needed to access a service, which in turn depended greatly on physical distribution of bandwidth and access points.[17]

---

[15] Cai, Hirtle, and Williams, "Mapping the Geography of Cyberspace Using Telecommunications Infrastructure Information," 146.
[16] Cai, Hirtle, and Williams, "Mapping the Geography of Cyberspace Using Telecommunications Infrastructure Information," 149.
[17] Cai, Hirtle, and Williams, "Mapping the Geography of Cyberspace Using Telecommunications Infrastructure Information," 149,151.

From a strategic viewpoint, the physical location of components also links cyberspace's virtual character to its physical implementation. This parameter has two distinct influences. From a cyber-defense perspective, access to the hardware allows some technical operations and privileges that supersede remote commands. Thus, for instance, a local administrator could reboot a server or a router to change the configuration or install new software. On the contrary, data or services that would be physically spread worldwide would have a harder time recovering from a takeover. In addition, the physical location of servers, routers, and relays connect actions in the physical realm with cyber-effects. Thus, physically destroying some elements of cyberspace, in abstraction or in addition to cyber-actions, can produce effects on cyber-objectives.

Mitigating this initial map of geographic information, the manufacturers of the components of cyberspace, is also useful to the strategist. Indeed, the identification of hardware and software constituting the cyber-environment provides important information on the potential for backdoors and indication of the time needed to fix critical vulnerabilities. As previously noted, vulnerabilities can be either discovered through testing or created during the design. A privileged access to the design of critical elements of the architecture can thus provide the attacker with significant advantage. In addition, definitely fixing vulnerability usually requires an intervention from the company

having developed the product. Following the interests of the company, its priorities and political pressures, the time required to develop and provide a fix may vary greatly.

Like its physical counterpart, cyber-geography has a tremendous effect on forces and subsequently on strategy. It strongly influences strategies through its effects on forces. Indeed, cyber-geography defines the difficulty of access of offensive forces to the potential objective. Many canons of cyber-strategy consider cyberspace as an essentially flat environment where access is instantaneous, which is inaccurate. While authorized communication are almost instantaneous, getting over adverse geography requires time, exhausts friendly forces and increases the chances of detection.

Cyber-Strategies

Validity of Strategic Cyber-objectives: According to Chapter 2, strategic cyber-attacks may produce two categories of effects. In the short term, they may encourage the enemy to select one course of action instead of another. In the longer term, they may convince the enemy to review initial objectives. Nevertheless, to achieve this end, cyber-strategy must demonstrate its enduring ability to harm the enemy or to produce definitive damage.

The problem of producing enduring effects is secondary for other military domains. For instance, strategic bombing shows the victim that bombers are able to overcome national defenses and strike at will. The only limit to the destruction they create is self-restraint.[18] On the contrary, even painful cyber-attacks do not systematically produce such effects.

First, mere disruption can be perceived as a temporary harm that will not persist once the conflict is over. Therefore it may not weigh significantly in the enemy cost-opportunity calculation. Indeed, the temporary effects of disruption are a lesser harm compared to definitive political objective, whether it is the possession of a nuclear arsenal for Iran or, say, the independence of a Serbian province.

Second, cyber-disruptions and destructions through cyberspace do not always imply the capacity to cause more disruption or destruction in the future. Indeed, performing cyber-attacks requires unveiling the vulnerabilities that allow the attack.[19] The time needed to correct these vulnerabilities or implement mitigating measures, that is to say the time during which the enemy may feel helpless against further harm, defines the maximum length of cyber-coercive effect.

---

[18] Schelling, *Arms and Influence*, 2008, 129.

[19] Discussing the limits of cyber-attacks, a distinguished guest argued, cyber-attacks are painful but they usually do not last. In addition, after an attack, the enemy is stronger because he has the opportunity to correct the vulnerabilities exploited during the attack.

Therefore, for cyber-attacks to have direct enduring political effects, they should promise future hardship. A fictitious scenario of a successful coercive cyber-attack could be the following: country A attacks some critical state B service, for instance, military payrolls, or social security personal information. Country A replicates the data and software to perform the service, then destroys country B data, so that country B cannot recover until these data are returned, yet has the immediate proof of the effects of a non-compliance. This scenario is close to the strategies criminals actually use to blackmail companies: hacking into a server, they encrypt critical data (sometimes, system data) and provide the key against ransom.

Strategy of Cyber-Conflict: As I argued in Chapter 3, a paramount aspect of strategy aims at reducing the effects of enemy initiative. One option is to outmaneuver opponents, putting them in a situation where they are constantly trying to adapt to friendly attacks. Other possibilities include mitigating the effects of enemy action or influencing cost-benefit analysis.

The first option is inherently offensive while the others are defensive in nature, regardless of the strategic purpose. Given the *a priori* clear distinction between offensive and defensive forces in cyberspace it makes sense to examine these trends separately. Finally, a discussion on the prospects of offensive defense in cyberspace elaborates on the

opportunities for a global cyber-strategy, linking offensive and defensive strategies.

Cyber-Offensive—On *GlitchKriege*: As already pointed out, even more so in cyberspace than in any other medium, the duration of the effects of an attack and the enemy resources mobilized by it are critical to a strategically significant offensive action. It allows designing a comprehensive cyber-strategy, both mobilizing enemy forces and maximizing strategic effects.

The strategic challenge of cyber-attacks is to convert the offensive action into a strategic advantage whose duration is compatible with strategic or political expectations.

Time, John Sheldon suggested, may be of the essence.[20] The duration of the strategic effects of a cyber-attack depends on two variables. The first one is related to the actual effects of the cyber-attack. As long as the enemy operational forces have not identified, analyzed, and mitigated the effects of the attack, the target system cannot perform nominally and the objective effects of the attack persist. The second effect of cyber-attacks is related to the correction of the vulnerabilities exploited. As long as research forces (for technical vulnerabilities) and operational forces (for human vulnerabilities) have not corrected the

[20] Sheldon, "Toward a Theory of Cyberpower," 209.

vulnerabilities, similar attacks are still susceptible of affecting the enemy. This subjective effect can last much longer because the enemy may have limited ability to correct vulnerabilities.

A thorough understanding of these two temporary effects is paramount to cyber-strategy. A cyber-attack can have a direct effect on the strategic objective. In that case, the time the enemy will need to recover will determine the duration of the strategic effect. For instance, an attack on IADS will be strategically significant as long as the enemy won't have recovered (corrected some vulnerabilities or implemented stopgap measures).

Alternately, a cyber-attack can also be meant to divert enemy defensive resources in order to strike another center of gravity later. "Strategy," Clausewitz wrote, "uses the results of battles to achieve its objectives." Attacks harming social centers of interests or military effectiveness may not create direct military or political effects, but mobilize defense resources. Given that cyber-defense resources are not destroyed, merely immobilized, offensive cyber-strategy must be extremely dynamic.

A difficulty that may arise concerning this assessment is the lack of physical contact. Thus, an attacker will only have very little

information on the effectiveness of an attack or clues about the recovery.[21]

Cyber-Defense—Attrition Warfare or War of Movement?: The challenges of the defensive are very different in nature. The perimeter to protect, at the national level, is extraordinary wide and suggests that complete protection is hardly achievable. The purpose of cyber-defense, therefore, is to reduce the impact of enemy attacks through a multilayered organization aiming at optimizing the chances of detections and increasing systemic robustness, and exhaust enemy offensive cyber-forces.

Defending from cyber-attacks is indeed a tremendous task. Unlike in other mediums, perimeter defense is seldom possible and never sufficient. It is not possible to isolate portions of cyberspace and filter all incoming flow, for instance. Indeed, even secured infrastructures include some level of connectivity with the rest of cyberspace, through removable media or operator action, for instance. Therefore, even the secure infrastructure security expert Edward Amoroso described must consider the possibility of attacks from the inside.[22]

---

[21] Sheldon, "Toward a Theory of Cyberpower," 209. In a credible scenario, the author showed that uncertainty as to the effects of cyber-attacks may undermine their operational effectiveness and credibility.
[22] Amoroso, *Cyber-attacks*, 51–72.

Therefore, all the elements to defend have to embed some level of security.[23] Already a serious obstacle while defending a military system, this difficulty becomes overwhelming at the national level. Moreover, as Sheldon emphasized, cyberspace has not been developed with security as a primary concern.[24] Consequently, many of its communication protocols pose threats to cyber-security.

Finally cyber-defense at the national level faces a problem of dispersion of responsibilities and interests as well as a lack of global overview. As I have suggested, many relevant targets for strategic cyber-attacks are owned and operated by private entities. For states, a significant challenge is to provide to these entities a level of support adequate to its strategic significance.[25] Nevertheless, coordination does not always offer the level of unity of effort situations request. Security expert Joel Brenner wrote, "Neither the United States government nor private industry can defend the networks on which our economic and national security depend."[26] This pessimistic statement illustrates the extent of the cyber-defense challenge.[27]

---

[23] Amoroso, *Cyber-attacks*, 109–128.
[24] Sheldon, "Toward a Theory of Cyberpower," 213.
[25] A distinguished visitor contended, "It is necessary to adapt state organizations to reach the flexibility required by cyber-defense. Indeed, the transverse nature of cyberspace challenges the fragmented organization of bureaucracies" (Point 4, 10 characters of cyber-conflicts).
[26] Brenner, *America the Vulnerable*, 94.
[27] To solve this problem of responsibilities, Susan Brenner argued, informal integration of actors in charge of national defense, law enforcement and private companies is necessary. An embryonic implementation could be the network of Computer Emergency Response Teams. Susan W. Brenner, *Cyberthreats: The Emerging Fault Lines of the Nation State* (Oxford, UK: Oxford University Press, 2009), 236.

Despite all these difficulties, cyber-defense's primary purpose is to mitigate the operational and strategic effects of cyber-attacks. This negative objective, in Clausewitz words, requires a thorough understanding of the operational implications of cyber-attacks and contingency plans to face potential disruption.

The operational effects of a cyber-attack cannot always be inferred from the technical details of the attack. Indeed, many services are interconnected and the attack of one element of the local cyberspace—or even outside its perimeter—can have unexpected consequences. In addition, the link between a system in cyberspace and an operational function requires a good understanding of the function of this system in the wider operational structure as well as the contingency plans besides the system.[28]

Mitigating the effects of cyber-attacks requires preliminary planning. This encompasses the possible means that can compensate the failure of operational systems and examine the possible failure of common services. It also encompasses the hardening of friendly functional cyber-geography.

Cyber-defense also plays another strategic role in cyber-conflict. It absorbs offensive forces through the neutralization of enemy cyber-

[28] As I was a young officer in charge of the operational IT network of an exercise in 2000, a cyber-attack downed a server that was critical to the Air Control function. Yet, to my great surprise, the exercise went on and my team did not even have a phone call to report the failure. As I understood later, the air traffic control operators are trained to operate with radio only when the visualization system was broken and simply applied this procedure.

weapons. As suggested before, designing cyber-weapons mobilizes significant cyber-forces. Research forces have to investigate enemy structure and assets to discover vulnerabilities. Operational forces have to design the attack, highlighting not only the vulnerabilities they have identified but also their *modus operandi*. These efforts must therefore generate concrete, operational results to be worth the investment.

Cyber-defense can absorb a portion of this capital by generating ambiguity about the link between cyber-asset and operational function. A typical example is the honeynet. These are networks simulating a real, operational network. Their purpose is to attract enemy attackers in order to analyze their attacks and divert them from operationally more sensitive networks.[29]

Finally, Robert Pape described the escaping strategies that usually make coercive strategies fail. He argued, "Modern states can minimize their vulnerability to counter-civilian attacks by defense, evacuation of threatened areas and rapid adjustment to economic dislocation."[30] Similarly, if subject to strategic cyber-attacks, a state can design a strategy of diversification, isolate the critical portions of national economy and expect its citizens to adapt to attacks on individual assets.

---

[29] A good example of honey net on the Internet can be found in Mark Bowden, *Worm: The First Digital World War* (New York: Atlantic Monthly Press, 2011).
[30] Pape, *Bombing to Win*, 23.

Prospects of Active Defense or Counterattack—Linking Offense and Defense:

Counterattack is not possible *per se* in cyberspace: indeed, a cyber-attack cannot harm enemy offensive cyber-forces, because of their nature exposed earlier. Therefore, offensive actions can have defensive effects in two cases. First cyber-deterrence can set limits to enemy strategic cyber-attacks. In addition, following the nature of enemy force structure, cyber-attacks may divert forces that would be used offensively otherwise.

A first protection against strategic cyber-attacks is deterrence. The advent of nuclear weapons suggested that when a new offensive weapon appears without a quick emergence of adequate defense, deterrence naturally emerges as a possible defensive option. Similarly, a cyber-deterrence policy can reduce the impact of strategic cyber-attacks. Nevertheless, cyber-deterrence faces some additional challenges.

First, cyber-deterrence cannot consist solely of cyber-retaliation. Indeed, some countries do not rely as critically on cyberspace as Western nations do. In such cases, deterrence declaratory policy should encompass the possibility of a kinetic response to cyber-attacks.[31]

In addition, the identification and categorization of cyber-attacks is critical to a massive retaliation. As Kugler emphasized, cyber-deterrence is a credible answer to critical cyber-attacks only.[32] Now, as Fidler

---

[31] Richard L. Kugler, "Deterrence of Cyber Attacks," in *Cyberpower and National Security,* ed. Franklin Kramer, Stuart Starr and Larry Wentz (Dulles, VA: Potomac Books, 2009), 326.
[32] Kugler, "Deterrence of Cyber-attacks," 326.

brilliantly exposed, several problems arise to attribute an attack to a state.[33]

Connecting an attack to an individual (or group of individuals) is already tricky, but connecting individuals to states is even more so. Yet, Kugler argued, if the perpetrator expects political effects, cyber-attacks cannot be concealed. Therefore, although cyber-deterrence can only address the most critical category of cyber-attacks, its importance cannot be completely negated by the attribution problem.[34]

Another prospect for using cyber-offensive as a defensive means regards the principle of economy of forces. A major cyber-conflict cannot reasonably be ruled out, if anything else because of the principle of escalation Clausewitz described. Accordingly, states would wage all available cyber-resources into the fight. Both defensive and offensive resources would be used to their maximum possible extent.

Research forces, for instance, would have to share their capacities between trying to find new vulnerabilities in enemy systems, and analyzing enemy attacks to find a response. Similarly, neutral research forces (antivirus laboratories, international research) would probably be

---

[33] Fidler, "Inter Arm Silent Reges Redux? The Law of Armed Conflict and Cyber Conflict" Among other legal issues, the author emphasized two difficulties related to the attribution of illegal action. The first one is technical, because the link between a computer and the identity of the perpetrator must be proved. In addition, the characterization of the attack is equally problematic. It is indeed difficult to decide whether an attack is criminal (hence an individual initiative punished by domestic laws) or state-led (in that case, the state assumes responsibility of the offense).

[34] Kugler, "Deterrence of Cyber Attacks," 326.

overwhelmed by the number of new vulnerabilities, and would probably not take sides and limit their support to belligerents.

Similarly, operational forces would probably seek to optimize their actions. Despite the significant differences between attackers and defenders know-how, the basic technological knowledge is similar. Some level of flexibility between offensive and defensive forces would provide a significant advantage. Should this flexibility occur, cyber-attacks on critical enemy nodes may force them to dedicate more assets to defense, thereby reducing their offensive potential.

Grand Cyber-Strategy

Forms of Cyber-war: From the elements exposed above, war in cyberspace may take several forms. It may become an important component of state coercive strategy or act mostly in support of military action. Following the primacy of offense or defense, it may develop as a war of movement or on the contrary as a war of attrition. Finally, the prospect of *silent war* cannot be excluded.

As I have shown, it is of the attacker's interest to try to outmaneuver the enemy. On the contrary, it is in defender's interest to try to exhaust enemy offensive forces, thus seeking a war of erosion. Therefore, the stronger trend is likely to dictate the unfolding of cyber-war.

Furthermore, concealed attacks are ones that are not meant to have visible effects. Concealed attacks offer several benefits. First, their effects last as long as the enemy is not aware of them. As long as the attack has not been detected and analyzed, the underlying vulnerabilities are still available for other categories of attacks. Finally, these concealed attacks offer distinct political advantages, since unlike physical, visible attacks they don't have the political drawbacks of an ostensible use of violence.

Preparing for Cyber-conflicts: Grand strategy is the long term effort of states to shape a favorable environment, thereby increasing their power and advancing their interests. Power in cyberspace develops following two main components. The shaping of cyber-geography can take the form of commercial predominance and of the control of critical portions of the internet. The generation of cyber-forces includes growing a global expertise in cyberspace.

As I have argued, cyber-geography is susceptible to playing an important role in cyber-conflict. Shaping a favorable environment is therefore a decisive challenge for cyberpower. As I showed earlier, some components of cyber-geography provide decisive advantages both offensively and defensively.[35] States should therefore invest cyber-

---

[35] Franklin D. Kramer and Larry Wentz, "Cyber-Influence and National Security," in *Cyberpower and National Security,* ed. Franklin Kramer, Stuart Starr and Larry Wentz (Dulles, VA: Potomac Books, 2009), 343–361. The authors emphasized the importance

geography along two complementary lines. First, an adequate level of control of critical portions of cyberspace (and especially the Internet) is paramount to ensure cyber-security. For instance, national routing infrastructures and national naming systems should be subject to scrutiny.

In addition, the origins of the components of cyberspace induce a level of control—and therefore a military advantage in the case of conflict—that commands a thorough analysis. The strength of a country's cyber-industry contributes to cyberpower in two respects. First, it generates cyber-specialists the country can hire during a conflict, in relatively short notice.[36] Moreover, developing cyber-assets nationally offers an unequaled access to the design and provides a clear advantage in the research and fixing of vulnerabilities. Although owning an entirely nationally designed infrastructure is not realistic for most states, a dynamic risk mitigation process must highlight the elements that may be more vulnerable and secure the critical infrastructures accordingly.

Another component of grand strategy is the generation of forces. The generation of cyber-weapons cannot be completely generic, because it must take into account each particular enemy system. In addition, cyber-weapons have a limited lifespan. On the other hand, the knowledge

---

of developing infrastructures in cyberspace to facilitate US informational power in cyberspace.

[36] Early airpower advocates clearly linked military airpower with the level of development of aeronautic activities in the state. See William Mitchell, *Winged Defense the Development and Possibilities of Modern Air Power--Economic and Military* (Tuscaloosa, AL: University of Alabama Press, 2009), 98.

required to develop cyber-weapons and use them is critical and long to develop. A priority of grand strategy should therefore be to develop research and operational cyber-forces.

Research forces can take the form of expert centers. They should seek access to a wide variety of cyber-assets, but they should also develop the ability to correct the vulnerability of the country's most critical systems should it be necessary. Operational forces need to develop both their technological expertise and their operational knowledge. Indeed, as I have suggested, both attack and defense require a thorough understanding of the operational effects of an attack. This paramount link between technical attack and operational effects requires some familiarity with doctrine, procedures and habits.

Finally, cyber-forces should seek the maximum possible flexibility. Cyber-defense specialists, today, are mostly dedicated to a system—a local portion of cyberspace—that depends on their organization. In addition, cyber-attackers are usually distinct teams that seldom assist defense teams.

As I have suggested, the ability to assign cyber-experts following operational priorities could provide a significant advantage during a cyber-conflict. Although a total flexibility would be excessively hard to achieve, the training of cyber-warriors should prepare them to this end. At the military level, cyber-defense and cyber-attack teams must develop a shared knowledge and increase their coordination.

Conclusion

In "An Imperfect Jewel: Military Theory and the Military Profession," Harold Winton offered several functions a theory of war fulfills.[1] Although this framework did not motivate the intellectual journey that led to this theory or the structure of this paper, the categories he defined offer an elegant way to summarize the main elements of this theory for cyberspace strategy.

Define

"Theory's first task," Doctor Winton argued, "is to define the field of study under investigation."[2] The components of cyberspace and its limits deserved a clear definition, in part because many organization and academic works give a different meaning to cyberspace and subsequently to cyberspace strategy. There is no question about the technical nature of cyberspace; most of the debates focus on where cyberspace stops. Since this definition aimed at developing strategic principles in the domain, it made sense to consider cyberspace as the medium made of computing systems, communication devices and electromagnetic spectrum, but also to include the technical data that enable its functioning. On the contrary, information at large exceeds the focus of

---

[1] Harold R. Winton, "An Imperfect Jewel: Military Theory and the Military Profession," *The Journal of Strategic Studies* no. 34 (December 2011), 2.
[2] Winton, "An Imperfect Jewel," 2.

cyberspace strategy. Information and influence strategies take place in a variety of mediums and cyberspace is one of them.

In addition, the study of strategy was defined here as a link between political bargaining and the use of violence. This analysis was necessary to determine what kinds of objectives in cyberspace and subsequently what kinds of strategies may foster favorable political outcomes. To paraphrase military strategist Bernard Brodie, this paper addressed the grey area where military strategy and political objectives meet.[3]

Connect

In addition, Harold Winton added, "Theory connects the field of study to other related fields in the universe."[4] This theory has attempted to connect the study of cyberspace strategy with several other, more classical spheres of knowledge. First and most importantly, it has connected cyberspace strategy to the ancient study of military strategy. This connection seems obvious, but several scholars contend that the characteristics of cyberspace are so novel that it requires an entirely new theoretical foundation. On the opposite side, I have abstracted some very generic principles of classical military theory and tried to apply them to cyberspace. For sure, some of the concepts manipulated have required a

---

[3] Brodie, *Strategy in the Missile Age*, 7–8.
[4] Winton, "An Imperfect Jewel," 3.

thorough redefinition in cyberspace. Nevertheless, this effort allows applying many principles of strategy in cyberspace.

This exercise also required analyzing some mechanisms of international relations. Indeed, the purpose of cyber-conflict being to achieve political effects, it was necessary to understand how violence can produce political effect to determine whether cyber-attacks fulfill these criteria and therefore to what extent strategic actions are relevant in cyberspace

Categorize

"The next task of theory is to categorize, i.e., to break the field of study into its constituent parts."[5] On this concern, this theory has disaggregated the strategic problem of cyberspace into several components. The cyber-objectives are the assets resting or connected to cyberspace, whose destruction or disruption produces military or political effects. The means of cyber-strategy, the cyber-forces, are the entities that generate, identify, exploit, mitigate, or correct vulnerabilities. They are either research forces or operational forces. Finally, cyber-geography is the most important factor of cyber-war. The structure of enemy and friendly cyberspace, its physical implantation, and the manufacturing origins of its constituting parts have a great influence on forces, their ability to reach their objectives, and therefore on cyber-strategy.

[5] Winton, "An Imperfect Jewel," 2.

Strategy itself can be divided into two complementary activities. Grand cyber-strategy aims at generating cyber-forces, optimizing their flexibility and at shaping a favorable cyber-geography. Cyber-strategy, on the other hand, uses these forces to overcome enemy cyber-forces and achieve cyber-objectives.

Explain

"Explanation is the soul of theory," Winton explained. Indeed, it is the most important function a theory provides; it is a rationally constructed body of knowledge. Fortunately, it is also the core of this paper. Thus, I emphasized, the instrumentality of violence resides in its ability to challenge enemy expected outcomes of conflict. Therefore, I elaborated, the logic of coercion exemplifies how violence achieves political objectives: it influences enemy cost-benefit analysis, making some enemy courses of action more unlikely or more costly. Consequently, the objectives of strategy are the elements of the enemy's military, society, and economy that either protect or host these centers of gravity. Accordingly, forces are all the means that can exert adequate pressure on these objectives. But not only enemy forces; the operational environment has a significant effect on forces in general. Thus, geography protects enemy centers of gravity, exhausts moving troops/forces, or provides a significant tactical advantage.

But strategy is more than a plan to coordinate resources to reach inert objectives. It requires overcoming a thinking and adapting enemy.

To reduce the effects of enemy unpredictability, strategy offers three generic solutions. Mitigating the effects of enemy action requires hardening friendly defenses and increasing their ability to recover from enemy attack. To reduce the range of enemy action, friendly strategy can alter enemy perception of the cost-benefit analysis of his strategy. Finally, the strategist can momentarily deprive the enemy of strategic options and put him on the defensive. Seizing and keeping initiative requires understanding the time enemy forces need to adapt to friendly action. The synchronization of these offensive moves allows keeping enemy forces under constant need for adaptation. This option requires a study of the dynamics of military forces and the time they need to adapt to friendly attacks or to their operational environment.

This framework is fully adaptable to cyberspace strategy. As I demonstrated, the definition of cyber-objectives, cyber-forces, and cyber-geography stem from their generic characterization. Therefore, these principles of static defense, initiative and deterrence fully apply in cyberspace.

Anticipate

"Finally, theory anticipates. In the physical realm, theory predicts, but action and reaction in the human arena, and therefore in the study of war, are much less certain; and I must be content to live with a lesser

standard."[6] This study provided tools for the cyber-strategist to anticipate the unfolding of conflict in cyberspace. Thus, the tenets of offense have been argued, and the prospects of active defense have been assessed. In addition, the paper extrapolated several possible developments of cyber-war following the predominance of attack or defense. Finally, the study suggested ways for states to prepare adequately its assets and environment for future cyber-conflict.

Way ahead?

This study barely laid the foundations for a theory of cyberpower, let alone fully explained all the intricacies of cyber-strategy. Many aspects have been left undeveloped. For instance, principles of strategy such as mass and economy of forces would have interesting applications according to the model offered. Similarly, this study disregarded several aspects of information warfare, at the operational and at the strategic level. Another lack stems from my choice to consider war as a bilateral issue. In every war, states and non-state actors have contradictory interests and postures, ranging from neutrality to partial support (provision of weapons, volunteers) to a full engagement. The role of third parties is especially important in cyberspace, in part because of geographic issues discussed above, but also neutral forces, like antivirus

[6] Winton, "An Imperfect Jewel," 3.

labs, play an important role in the detection and correction of vulnerabilities in peacetime.

At claimed in the introduction, the first major conflict involving massive struggle in cyberspace is yet to come. So far, cyber-attacks have plagued technologically (and cyber-savvy) countries but they have produced no significant political effect so far. Nevertheless, states have to prepare for this eventuality, if anything else because their increasing reliance on the medium commands to protect their valuable assets. In this domain, the security dilemma does not operate so bluntly. One can increase its national defense; develop its forces with limited risk to trigger an arms race. More than the increase in power, it is the use of cyber-force that spurs potential rivals to develop a cyber-arsenal.

BIBLIOGRAPHY

Air Force Doctrine Document. “AFDD 3-12, Cyberspace Operations,” July 15, 2010.

Allison, Graham T, and Philip Zelikow. *Essence of Decision : Explaining the Cuban Missile Crisis*. New York [etc.]: Longman, 1999.

Amoroso, Edward. *Cyber Attacks: Protecting National Infrastructure*. 1st ed. Burlington, MA: Butterworth-Heinemann, 2010.

Anderson, Ross, Chris Barton, Rainer Böhme, Richard Clayton, Michel JG van Eeten, Michael Levi, Tyler Moore, and Stefan Savage. “Measuring the Cost of Cybercrime.” In *11th Workshop on the Economics of Information Security (June 2012)*, 2012. http://lyle.smu.edu/~tylerm/weis12pres.pdf.

ANSSI/ACE/BAC. “EBIOS - Risk Management Method,” 25 2010.

Archives Nationales. “Compagnie Des Indes.” Accessed May 20, 2013. http://www.memoiredeshommes.sga.defense.gouv.fr/indes/.

Atran, Scott. *Talking to the Enemy: Faith, Brotherhood, and the (un)making of Terrorists*. New York: Ecco Press, 2010.

Baldwin, David A. *Economic Statecraft*. Princeton, NJ: Princeton University Press, 1985.

Beaufre, André. *Introduction à La Stratégie*. [Paris]: Pluriel, 2012.

———. *Introduction à la Stratégie*. Paris: Pluriel, 2012.

Berry, Daniel M. “Formal Methods: The Very Idea: Some Thoughts About Why They Work When They Work.” *Science of Computer Programming* 42, no. 1 (2002): 11–27.

Betz, David J., and Tim Stevens. *Cyberspace and the State: Toward a Strategy for Cyber-power*. 424. London, UK: The International Institute for Strategic Studies, 2011.

Biddle, Tami Davis. *Rhetoric and Reality in Air Warfare: The Evolution of British and American Ideas About Strategic Bombing, 1914-1945*. Princeton, NJ: Princeton University Press, 2002.

Bousquet, Antoine. *The Scientific Way of Warfare: Order and Chaos on the Battlefields of Modernity*. India: Columbia University Press, 2009.

Bowden, Mark. *Worm: The First Digital World War*. New York: Atlantic Monthly Press, 2011.

Brenner, Joel. *America the Vulnerable: Inside the New Threat Matrix of Digital Espionage, Crime, and Warfare*. New York: Penguin, 2011.

Brenner, Susan W. *Cyberthreats: The Emerging Fault Lines of the Nation State*. Oxford, UK: Oxford University Press, 2009.

Brodie, Bernard. *Strategy in the Missile Age*. Santa Monica, CA: Rand Corp., 2007.

Bueno de Mesquita, Bruce. *The War Trap*. New Haven, CT: Yale University Press, 1981.

Builder, Carl H. *The Masks of War: American Military Styles in Strategy and Analysis*. Baltimore: Johns Hopkins University Press, 1989.

Cai, Guoray, Stephen Hirtle, and James Williams. “Mapping the Geography of Cyberspace Using Telecommunications Infrastructure Information.” *TeleGeo* (1999): 6–7.
Chemel, Edouard. *Chronique de l’aviation.* Paris: Éditions Chronique Acropole, 1991.
Clarke, Richard A, and Robert K Knake. *Cyber War: What It Is and How to Fight It*. New York: Ecco, 2010.
Clarke, Richard A., and Robert Knake. *Cyber War: The Next Threat to National Security and What to Do About It*. New York: HarperCollins, 2010.
Clausewitz, Carl von. *On War*. Translated and edited by Michael Howard and Peter Paret. Princeton, NJ: Princeton University Press, 1984.
Clausewitz, Carl von. *On War*. Princeton, N.J.: Princeton University Press, 1984.
———. *On War*. Princeton, N.J.: Princeton University Press, 1984.
Clodfelter, Mark. *The Limits of Air Power: The American Bombing of North Vietnam*. Lincoln, NE: University of Nebraska Press, 2006.
Coutau-Bégarie, Hervé. *Traité de Stratégie*. 5e éd. rev. et augm. Bibliothèque Stratégique. Paris: Institute de Stratégie Comparée : Economica, 2006.
Coutau-Bégarie, Hervé. *Traité de stratégie*. Paris: Institut de stratégie comparée : Économica, 2006.
Dicken, Peter. *Global Shift: Mapping the Changing Contours of the World Economy*. New York: Guilford Press, 2011.
Dolman, Everett C. *Pure Strategy : Power and Principle in the Space and Information Age*. New York: Frank Cass, 2005.
———. *Pure Strategy : Power and Principle in the Space and Information Age*. London; New York: Frank Cass, 2005.
Douhet, Giulio. *The Command of the Air*. Tuscaloosa, Ala.: University of Alabama Press, 2009. http://site.ebrary.com/id/10527828.
———. *The Command of the Air*. Fire Ant Books. Tuscaloosa, AL: University of Alabama Press, 1998.
Fidler, David P. “Inter Arm Silent Reges Redux? The Law of Armed Conflict and Cyber Conflict.” In *Cyberspace and National Security*, edited by Derek S. Reveron, 71–87. Georgetown University Press. Wahington, DC, 2012.
Floridi, Luciano. “The Future Development of the Information Society.” *Jahrbuch Der Akademie Der Wissenschaften in Göttingen* (2007): 175–187.
Galula, David. *Pacification in Algeria, 1956-1958*. Santa Monica, CA: RAND Corporation, 2006.
Giddens, Anthony. *A Contemporary Critique of Historical Materialism. Vol. 2, The Nation-state and Violence*. Los Angeles,CA: University of California Press, 1987.

Gray, Colin. *Strategy for Chaos: Revolutions in Military Affairs and the Evidence of History*. London, UK: Franck Cass, 2002.
Griffith, Samuel B. "Preface." In *The Illustrated Art of War*, translated by Samuel B. Griffith. New York: Oxford University Press, 2005.
Growth, Competitiveness, Employment: The Challenges and Ways Forward into the 21st Century: White Paper. Bulletin of the European Communities. Supplement 6/93. Luxembourg: Office for Official Publications of the European Communities ; UNIPUB, distributor], 1993.
Hadnagy, Christopher. *Social Engineering: The Art of Human Hacking*. Indianapolis, IN: Wiley Publishing Inc., 2010.
Hazewinkel, Michiel. *Encyclopaedia of Mathematics*. Berlin; New York: Springer-Verlag, 2002.
Henriksen, Dag. *Nato's Gamble: Combining Diplomacy and Airpower in the Kosovo Crisis, 1998-1999*. Annapolis, MD: Naval Institute Press, 2007.
Holmes, Richard. *The Oxford Companion to Military History*. Oxford; New York: Oxford University Press, 2004.
Horne, Alistair. *A Savage War of Peace: Algeria, 1954-1962*. New York: New York Review Books, 2006.
Iklé, Fred Charles. *Every War Must End*. New York: Columbia University Press, 2005.
Joint Publication Document. "JP3.13 Joint Doctrine for Information Operations," November 27, 2012.
Jomini, Antoine Henri. *The Art of War*. Mineola, NY: Dover Publications, 2007.
Jones, Marcus. "Strategy as Character: Bismarck and the Prusso-German Question, 1862-1878." In *The Shaping of Grand Strategy: Policy, Diplomacy, and War*, edited by Williamson Murray, Richard Hart Sinnreich, and James Lacey. New York: Cambridge University Press, 2011.
Kalyvas, Stathis N. *The Logic of Violence in Civil War*. Cambridge Studies in Comparative Politics. New York: Cambridge University Press, 2006.
Khong, Yuen Foong. *Analogies at War: Korea, Munich, Dien Bien Phu, and the Vietnam Decisions of 1965*. Princeton, NJ: Princeton University Press, 1992.
Kilcullen, David. "Countering Global Insurgency." Edited by Thomas G Mahnken and Joseph A Maiolo. *Journal of Strategic Studies* 28, no. 4 (2005): 597–617.
Kramer, Franklin D. "Cyberpower and National Security: Policy Recommendations for a Strategic Framework." In *Cyberpower and National Security*, edited by Franklin D. Kramer, Stuart H Starr, and Larry K Wentz. Washington, DC: Potomac Books, 2009.

Kramer, Franklin D., Stuart H Starr, and Larry K Wentz, eds. *Cyberpower and National Security: Policy Recommendations for a Strategic Framework*. Washington, DC: Potomac Books, 2009.
Kramer, Franklin D., and Larry Wentz. "Cyber Influence and Nationsl Security." In *Cyberpower and National Security*, 343–361. Dulles, VA: Potomac Books, 2009.
Kuehl, Daniel. "From Cyberspace to Cyberpower: Defining the Problem." In *Cyberpower and National Security*, edited by Franklin D. Kramer, Stuart H. Starr, and Larry Wentz, 24–42. Dulles, VA: Potomac Books, Inc., 2009.
Kugler, Richard L. "Deterrence of Cyber Attacks." In *Cyberpower and National Security*, 309–340. Dulles, VA: Potomac Books, 2009.
Lambeth, Benjamin S. *The Transformation of American Air Power*. Ithaca, NY: Cornell Univ. Press, 2000.
Leiner, Barry M., Vinton G. Cerf, David D. Clark, Robert E. Kahn, Leonard Kleinrock, Daniel C. Lynch, Jon Postel, Larry G. Roberts, and Stephen Wolf. "A Brief History of the Internet" (1999). http://arxiv.org/abs/cs/9901011.
Libicki, Martin C. *Conquest in Cyberspace: National Security and Information Warfare*. New York: Cambridge University Press, 2007.
———. "Sub Rosa Cyber War." *The Virtual Battlefield: Perspectives on Cyber Warfare* 3 (2009): 53.
Liddell Hart, Basil Henry. *Strategy*. New York: Meridian, 1991.
Lonsdale, David J. *The Nature of War in the Information Age : Clausewitzian Future*. Portland, OR: Frank Cass, 2004.
Lonsdale, David J. *The Nature of War in the Information Age: Clausewitzian Future*. New York: Frank Cass, 2004.
Mahan, A. T. *Mahan on Naval Strategy: Selections from the Writings of Rear Admiral Alfred Thayer Mahan*. Annapolis, MD: Naval Institute Press, 1991.
Major General Brett T. Williams. Cyber Operations, 06 2013.
McNeill, William H. *The Pursuit of Power: Technology, Armed Force, and Society Since A.d. 1000*. Chicago, IL: University of Chicago Press, 1984.
"Merriam-Webster's Collegiate Dictionary." Springfield, MA: Merriam-Webster, Inc., 2008.
Mitchell, William. *Winged Defense the Development and Possibilities of Modern Air Power--Economic and Military*. Tuscaloosa, AL: University of Alabama Press, 2009.
Mizrach, Steve. *Lost in Cyberspace: a Cultural Geography of Cyberspace*. Steve Mizrach, 1996. http://www2.fiu.edu/~mizrachs/lost-in-cyberspace.html.
Moltke, Helmuth. *Moltke on the Art of War: Selected Writings*. Translated and edited by Daniel J. Hughes. Novato, CA: Presidio Press, 1995.

Morozov, Evgeny. *The Net Delusion: The Dark Side of Internet Freedom*. New York: PublicAffairs, 2012.
Murray, Williamson. "Operation Iraqi Freedom, 2003." In *A History of Air Warfare*. Potomac Books, 2010.
Osinga, Frans P. B. *Science, Strategy and War : the Strategic Theory of John Boyd*. New York: Routledge, 2007.
Pape, Robert Anthony. *Bombing to Win: Air Power and Coercion in War*. Ithaca, NY: Cornell University Press, 1996.
Reveron, Derek S., ed. *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World*. Washington, DC: Georgetown University Press, 2012.
Rid, Thomas, and Marc Hecker. *War 2.0 : Irregular Warfare in the Information Age*. Westport, Conn.: Praeger Security International, 2009.
Schelling, Thomas C. *Arms and Influence*. New Haven, Conn.; London: Yale University Press, 2008.
Schelling, Thomas C. *Arms and Influence*. New Haven, CT: Yale University Press, 2008.
Schmitt, Eric. *Counterstrike: The Untold Story of America's Secret Campaign Against Al Qaeda*. 1st ed. New York: Times Books, 2011.
Sheldon, John B. "Toward a Theory of Cyberpower." In *Cyberspace and National Security*, edited by Derek S. Reveron, 207–224. Washington, DC: Georgetown University Press, 2012.
Shwedo, Bradford J. *XIX Tactical Air Command and ULTRA: Patton's Force Enhancers in the 1944 Campaign in France*. CADRE Paper no. 10. Maxwell Air Force Base, AL: Air University Press, 2001.
Singh, Simon. *The Code Book : the Secret History of Codes and Code-breaking*. London, UK: Fourth Estate, 2000.
Sinnreich, Richard Hart. "Patterns of Grand Strategy." In *The Shaping of Grand Strategy: Policy, Diplomacy, and War*, edited by Williamson Murray, Richard Hart Sinnreich, and James Lacey, 254–269. New York: Cambridge University Press, 2011.
Starr, Stuart H. "Toward a Preliminary Theory of Cyberpower." In *Cyberpower and National Security*, edited by Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz, 43–88. Washington, D.C.: Potomac Books, 2009.
Sun Tzu. *The Illustrated Art of War*. Translated by Samuel B. Griffith. New York: Oxford University Press, 2005.
"The Impact of WWI on the Course of American Radio History." Accessed February 20, 2013. http://www.academia.edu/937415/The_Impact_of_WWI_on_the_Course_of_American_Radio_History.
Thomas, Timothy L. "Nation-state Cyber Strategies: Examples from China and Russia." In *Cyberpower and National Security*, edited by

Stuart H. Starr, Larry K. Wentz, and Franklin D. Kramer. Washington, D.C.: Potomac Books, 2009.
Tooze, J. Adam. *The Wages of Destruction: The Making and Breaking of the Nazi Economy*. New York: Penguin USA, 2008.
Tse-Tung, Mao. "On Protracted War," May 1938. http://www.marxists.org/reference/archive/mao/selected-works/volume-2/mswv2_09.htm.
Villatoux, Paul, and Marie-Catherine Villatoux. *La République et Son Armée Face Au Péril Subversif: Guerre et Action Psychologiques En France, 1945-1960*. Les Indes savantes, 2005.
Waltz, Kenneth Neal. *Theory of International Politics*. Long Grove, Ill.: Waveland Press, 1979.
———. *Theory of International Politics*. Long Grove, IL: Waveland Press, 1979.
Williams, Brett T. "Ten Propositions Regarding Cyberspace Operations." *Joint Forces Quarterly*, quarter 2011.
Winton, Harold R. "An Imperfect Jewel: Military Theory and the Military Profession" (n.d.).
———. "An Imperfect Jewel:Military Theory and the Military Profession." *The Journal of Strategic Studies* no. 34 (December 2011).
Wolk, Herman S. *Cataclysm: General Hap Arnold and the Defeat of Japan*. Denton, TX: University of North Texas Press, 2010.
Wright, Quincy. *A Study of War*. Chicago, IL: University of Chicago Press, 1965.
Wylie, J. C. *Military Strategy: a General Theory of Power Control*. Annapolis, Md: Naval Institute Press, 1989.
Wylie, Joseph C. *Military Strategy: A General Theory of Power Control*. Classics of Sea Power. Annapolis, MD: Naval Institute Press, 1989.